Volume I Issue 2 Winter 2013

Cyber PCE Compendium

Cyber 300 Professional Continuing Education
CCR-TR-2013a-Vol-1-No-2

Dr. Harold Arata III, Mr. Juan Lopez Jr., Lt Col John Bommer Jr. (eds.)

Air Force Cyberspace Technical Center of Excellence
Center for Cyberspace Research
Air Force Institute of Technology
2950 Hobson Way
Wright-Patterson AFB, OH 45433

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
16 DEC 2013	**Summary**	**01 JUL 2013 - 31 DEC 2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber PCE Compendium:Cyber 300 Professional Continuing Education	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Editors: Dr. Harold Arata III, Juan Lopez Jr., & Lt Col John Bommer Jr.	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Cyberspace Technical Center of Excellence, Center for Cyberspace Research, Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson AFB, OH 45433	**CCR-TR-2013a-Vol-1-No-2**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
Published twice annually., The original document contains color images.

14. ABSTRACT

This compendium represents a select collection of deliberate thoughts, strong opinions, and conscientious commentaries from students attending the Cyber 300 course at the Air Force Institute of Technology. The range of topics covers a myriad of technical and non-technical issues that are often compounded by the cyber domain, address challenges and potential solutions experienced by leaders across the enterprise. The contributing authors represent a broad pedigree of professionals across the enterprise that includes all military departments (active duty, guard, and reserve components), officers, civil service, enlisted personnel, and allied partners (Great Britain, Australia, and Canada). The position papers will in some cases be rather controversial and provoke thought. In the end, the intent is to make these contributions a basis for encouraging discussion and actions, leading to the development of techniques, tactics, and procedures that advance topics relevant to cyberspace.

15. SUBJECT TERMS
Cyber 300, PCE COmpendium, Cyberspace, Cyber Policy,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**172**	

Contents

DIRECTORS FOREWORD

Welcome to the Winter 2013 issue of the *Cyber PCE Compendium*, a new publication by cyberspace professionals for the growing community of professionals interested in cyberspace, particularly the cyberspace domain relative to military operations.

On 19 June 2008, the Secretary and Chief of Staff of the Air Force designated the Air Force Institute of Technology and the Center for Cyberspace Research as the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE). The AF CyTCoE is chartered to be a unifying and synergistic body for promoting cyberspace education, training, research, and technology development. The AF CyTCoE facilitates development of Air Force education and training in support of cyberspace operations as well as identifies and provides subject matter experts who understand doctrine, techniques, and technology to ensure dominance in cyberspace.

Based on the SECAF and CSAF directed mission and the research, education, and technical credentials of the AF CyTCoE, the Center was tasked to develop educational courses that enable cyberspace operators, regardless of specialty, to adapt to the quickly changing cyberspace environment. To this end, the AF established the cyberspace senior and master certification courses, Cyber 200/300. Since their inception, both courses have undergone considerable revision, institutional review, and have been granted Joint certification and Allied approval.

Cyber 300 is a certification course for cyberspace professionals transitioning from intermediate to higher-level responsibilities. Cyber 300 students are provided a broad background in cyber concepts, including capabilities, limitations, vulnerabilities, and the associated application and employment of cyberspace options in joint military operations. A fundamental component of the educational process is to encourage critical thinking and provoke thought that will push knowledge barriers beyond the edges that collectively contain the current art of the possible.

This compendium represents a select collection of deliberate thoughts, strong opinions, and conscientious commentaries from students attending the Cyber 300 course. The range of topics cover a myriad of technical and non-technical issues that are often compounded by the cyber domain, address challenges and potential solutions experienced by leaders across the enterprise.

Please enjoy our newest issue of the cyber compendium!

HAROLD J. ARATA III, PhD
Director, Air Force Cyberspace
Technical Center of Excellence
Center for Cyberspace Research

OVERVIEW

This compendium provides a select collection of position papers generated by students attending the Cyber 300 Professional Development Course hosted by the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE) at the Air Force Institute of Technology (AFIT). The position-paper construct aptly enables discussion on emerging cyber topics without the rigor of experimentation and original research normally required for publication in an academic publication. The now familiar and recognized rapid momentum in the cyber domain makes it prudent to capture and distribute emerging philosophy and opinions related to cyber warfare specific to military operations.

This compendium provides a reference source and living repository on a wide variety of cyber topics that address the unique applications of the military professional. This compendium will be refreshed semi-annually to preserve the content and resist staleness. Furthermore, the publication will maintain a persistence presence online through the services offered by the Defense Technical Information Center (DTIC).

The contributing author's represent a broad pedigree of professionals across the enterprise that includes all military departments (active duty, guard, and reserve components), officers, civil service, enlisted personnel, and allied partners (Great Britain, Australia, and Canada). The position papers will in some cases be rather controversial and provoke thought. In the end, the intent is to make these contributions a basis for encouraging discussion and actions, leading to the development of techniques, tactics, and procedures that advance topics relevant to cyberspace.

TOPIC COVERAGE

We live in a world of technological innovation and discovery. Technology forecasting is an important element of managing information technology risks. Any organization dependent on information technology realizes that managing risk associated with technology is a difficult endeavor. The connectivity of Department of Defense (DOD) information systems and information technology-dependent warfighting platforms to DOD networks and the Internet offers exploitation opportunities and continues to present a serious risk.

The topic selection process is guided by 27 specific questions generated by the senior leadership at Headquarters Air Force in collaboration with other DOD agencies. The students attending the professional continuing education course are presented with these questions during a brain storming session and provided the time and opportunity to formulate a thoughtful response and present it as a position paper. The aggregation of those responses are captured in this volume and provided to the reader for consideration of their merits. The position papers are clustered under a single theme that represents the core topic being discussed. The themes are designed to allow them to change over time in order to mimic the rapidly changing landscape of cyberspace. It is our sincere hope that this collaborative effort will incite further discussion and expedite forethought in strategy development from the next generation of cyberspace leaders.

THE CENTER FOR CYBERSPACE RESEARCH AND THE AIR FORCE CYBERSPACE TECHNICAL CENTER OF EXCELLENCE

In the mid-1990s, Department of Electrical and Computer Engineering (ENG) faculty at the Air Force Institute of Technology (AFIT) began developing and teaching courses in computer networks and information operations. These courses allowed students to gain expertise in emerging technology areas highly relevant to the mission of the United States Air Force. The computer network courses covered the theory and technologies behind the evolution of the infrastructure we now call the Department of Defense Information Network (DODIN). The information operations sequence covered emerging threats associated with the use of information in a computer age. This included how malicious software can be developed and deployed to exploit inherent vulnerabilities associated with systems used within the DOD.

In 2001, AFIT applied for recognition as a National Center of Academic Excellence in Information Assurance Education (CAE-IAE), sponsored by the DOD and administered by the National Security Agency (NSA). AFIT was designated a CAE-IAE in March 2002. At the time of this designation, only 12 schools across the country held this status. As a result of this designation, AFIT began to participate in the Information Assurance Scholarship Program (IASP) operated by the DOD and administered by the NSA to place military and DOD civilian students into school to gain Information Assurance-related degrees. In the spring of 2002, the AFIT Center for Information Security Education and Research (CISER) was founded. At its' inception, three ENG faculty members (Dr. Raines, Dr. Baldwin, and Dr. Gunsch) formed the core of CISER. These faculty members began to grow and expand AFIT's role in this area of education and research. As part of this expansion and growth, a Distinguished Review Board (DRB) was established to help oversee the progress on the CISER.

In 2004, AFIT approved a Master of Science degree program in Information Assurance resulting from the growth in the area and increased interest in information-security related education. In 2005, AFIT was re-designated as a CAE-IAE for 3 years and also received a grant from the National Science Foundation (NSF) to fund Scholarship for Service fellowships for five students to pursue information assurance-related degrees and then work for the US Federal Government upon completion of their programs.

In 2006, a 12-month Master's Degree program in Cyber Warfare was established as an Intermediate Development Education program for field-grade officers. The first cadre of 12 students arrived in June 2007.

In April 2007, as a result of input from Headquarters Air Force, the CISER changed its name to the Center for Cyberspace Research (CCR) to more closely align with the Air Force mission in cyberspace. Also in 2007, and as a result of direction from the center's Distinguished Review Board and operational Air Force input, the Master's Degree program in Information Assurance underwent a name change to Master of Science (Cyber Operations).

Since 2005, the CCR has worked closely with Headquarters Air Force Space Command and 24th Air Force (AFCYBER) to move towards the force development of personnel with technical skill sets required to operate in the cyberspace warfighting domain. This close working relationship CCR fostered has required an expanded role for the CCR beyond its traditional graduate education and research mission. For example, the CCR was tasked to assist Air University with the integration of cyberspace techniques and concepts into the Professional Military Education programs.

As a result of CCR initiatives, research and close interactions across the Air Force, in June 2008, the Secretary of the Air Force designated AFIT and the CCR as the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE). The charter of the AF CyTCoE is to bring a level of understanding to the Air Force on "who is doing what in cyberspace." This charter includes education, graduate research, and outreach initiatives to ensure efficiency of operations and to promote partnerships between government, industry, and academia. During this period, Dr. (then Colonel) Arata joined the AF CyTCoE as a founding member and a Cyberspace Education Board of Advisors (BOA) was established to oversee the progress of the AF CyTCoE. Also in 2008, AFIT and the CCR were re-designated as a CAE-IAE. In late 2008, the CCR was tasked by Headquarters Air Force to lead the cyberspace Professional Continuing Education development efforts based on demonstrated leadership and technical capabilities.

In 2009, the CCR received a new designation from NSA-DHS as a CAE-IAE-R. This recognizes CCR's research role in the cyberspace domain. At the time of designation, only 22 academic institutions from across the country held a similar designation. At the present time, the CCR has over 20 active faculty members and annually conducts 40-50 research efforts. The CCR has eight active research laboratories spanning critical infrastructure, computer network exploitation and attack, wireless networking and security, malicious code analysis, and software assurance/protection. With the research generated within CCR, the Air Force-level Center is able to proudly produce the Air Force's new cyber operators.

HISTORY OF CYBER 200/300

The Air Force Cyberspace Technical Center of Excellence (AF CyTCoE) was stood up at the Air Force Institute of Technology (AFIT) under the leadership of AFIT's Center for Cyberspace Research (CCR) in June 2008 by the Secretary of the Air Force (SECAF) and the Chief of Staff of the Air Force (CSAF) to "develop and maintain a cadre of professionals who can fight offensively and defensively in cyberspace" and to "develop relationships with and maintain awareness about the activities of various cyber-related research, education, and training communities within the Air Force, our service partners in the DOD, various federal agencies, and civilian academic and commercial research organizations across the globe."

CCR was specifically selected because it had been doing just that since 2002. In addition to the SECAF and CSAF designation in 2008, the CCR has been competitively selected for several honors and "Center of Excellence" designations, including:

- NSA/DHS Research Center of Excellence
- NSA/DHS Center of Academic Excellence in Information Assurance Education
- National Science Foundation designated Center
- Placed first in 8 of the last 10 years in annual NSA-sponsored Cyber Defense Exercise
- 1st place DOD Cyber Crime Center Digital Forensics Challenge, 2007 and 2009

Other Center honors and awards include:

- 2008 and 2010 Air Force Science/Engineering Educator Year Award
- 2008 Air Force Junior Scientist of the Year Award
- 2010 IEEE National Outstanding Elec/Computer Eng Teacher Award
- 2010 Ralph J. Mastrandrea Research Contributions Award
- 2011 Government Information Security Leadership Award (Workforce Improvement)—Cyber 200/300
- 2011 AETC Info Dominance (Cyber Ops) Award
- 2011 Fellow of the Information Systems Security Association
- 2011 Fellow, National Board of Information Security Examiners
- 2012 Government Information Security Leadership Award Finalist (Workforce Improvement)—ACE development & delivery
- 2012 AETC National Public Service Award
- 2012 AF STEM Senior Military Engineer Year Award
- 2012 Ohio Governors "Distinguished Hispanic Ohioan Award" for Research Excellence and STEM Community Outreach
- 2013 AF Research and Development Year Award
- 2013 AETC STEM Senior Military Engineer Year Award
- 2013 AETC Outstanding Scientist-Mid Career Military Year Award
- 2013 AETC Outstanding Engineer Team Year Award
- 2013 AETC Research Management Year Award
- 2013 AETC General Wilma Vaught Visionary Leadership Award
- 2013 AETC Info Dominance Outstanding Cyberspace Systems SNCO
- 2013 AETC Info Dominance Outstanding Information Assurance Element

Based on these credentials and the SECAF-directed mission, SAF/CIO A6 formally tasked the AF CyTCoE to develop educational courses that would enable the cyber workforce, regardless of specialty, to adapt to the quickly changing environment. Soon after, Air Education and Training Command, under the leadership of General Stephen Lorenz, directed the AF CyTCoE to host and execute the courses by October 2010 (FY11). Air University (under Lt Gen Allen Peck), as the education arm of AETC, recommended the AF CyTCoE at AFIT as the permanent location on 12 March 2010 based on several factors, such as proximity to AF cyber research (AFRL), acquisition (AFMC/AFLCMC), intelligence (NASIC), and combat communications units, low travel and per diem costs, and existing cyber educational facilities. On 2 April 2010, AETC formally announced AFIT as the permanent location for the Cyber 200 and Cyber 300 courses. Furthermore, the SECAF, in April 2008, and most recently the VCSAF in August 2010, called out Cyber 200/300 as a formal requirement for the Air Force via the Air Force Roadmap for Development of cyberspace Professionals. The Quadrennial Defense Review also called for DOD to grow a cadre of cyber experts to protect and defend information networks in Feb 2010.

COMPENDIUM CONTRIBUTORS

- Harold J. Arata III, PhD
- Lt Col John S. Bommer Jr.
- Major Frederic W. Lunas
- Major Jeffery A. Naylor
- Major Stacie A. Rembold
- Major Richard B. Shoaf
- Capt Scott L. Anderson
- Capt Kristen L. Engle
- CW4 Elbert W. Peak
- MSgt Carlos J. Frevert
- MSgt Eleanor D. Blystone
- Mr. Juan Lopez Jr.
- Mr. Brian L. Hale
- Ms. Carrie Solberg

PART I: TACTICS

Recommendations for Cyber Risk Management Framework
LTC Michael L. Haggard, U.S. Army (Network Enterprise Technology Command)

ABSTRACT

Cyber threats are increasing daily and require enduring vigilance to maintain secure, mission ready networks. However, Army senior leaders still experience challenges relating the often technically esoteric cyber risk with a risk to mission assurance. Therefore, it can be difficult to compel mitigating actions, especially if those mitigations interfere with operators conducting their missions. To overcome these challenges, this paper proposes a risk management framework that starts with Boyd's Observe-Orient-Decide-Act (OODA) loop and incorporates a risk assessment formula comparing threat actions, vulnerabilities, and mission assurance asset priority against potential countermeasures. In order to effectively translate the arcane technical jargon into a range of countermeasures senior leaders can understand, cyber operators must match threat actors to current network vulnerabilities and develop a level of risk against specific mission assurance assets. The analysis then needs to develop risk-based courses of action for leaders to accept, avoid, mitigate, share, or transfer. If the leader wants to mitigate, share, or transfer the risk, then cyber operators can provide specific countermeasures required to limit the threat actors' freedom of action in cyberspace. Finally, the paper will explain why this risk management framework is important, even as the Army has already implemented many countermeasures.

DESCRIPTION OF ISSUE

1. While the Army's LandWarNet (LWN) is an integral part of Army Operations; current Army doctrine describes it as a battlefield-enabler rather than a domain.[1] Yet, with the advent of cyberspace and considerations of cyber power, LWN has transformed into a contested domain in 'which and through' the U.S. Army and federal government can achieve national-defense goals. However, the ability of cyberspace to bridge traditional military domains and national centers of gravity through interconnectivity has created new avenues for the threat to influence American interests. As noted by Lieutenant General (LTG) Rhett Hernandez, Commanding General (CG), U.S. Army Cyber Command/2nd Army (ARCYBER) in his remarks to the House Armed Services Committee (HASC), the threat is varied, sophisticated, evolving, and dangerous. Their increasing ability to disrupt networks or critical infrastructure impacts the Army's freedom of operation in cyberspace and creates a "dynamic and dangerous cyberspace environment."[2] However, the U.S. Army is not operating in this contested domain as well as it could, in part because of a lack of a focused, structured cyber risk management framework.

2. The first element hampering risk assessment in cyberspace is the lack of a comprehensive threat analysis that can account for threat capabilities and intent. In 2011, the Center for Strategic Leadership (CSL) at the U.S. Army War College (USAWC) hosted a Cyberspace Operations Workshop to explore what facets of information Army senior leaders require to become "cyber-aware." The Threat and Vulnerability Work Group stated, senior leaders understand threat descriptions revealing a pattern of constant probing, infiltration, data compromise, and even physical damage."[3] This illustrates the need to describe the cyberspace domain in operational terms to enable senior leaders to fully appreciate the capability of the threats' ability to affect mission assurance 'in and through' cyberspace. The CSL study further reported that senior leaders prefer to have specific vignettes that clearly explain the nature of the threat and the relationship between attacks and vulnerabilities. The following four methods used to consider

threats (1) Threat Payload and/or Effect, (2) Threat Originators, (3) Threat Strategies, and (4) Means-Motive-Opportunity[4] indicates that cyber operators focus on framing their discussions in similar terms to effectively align threats-to-cyberspace capabilities with threats-to-mission assurance.

3. In addition to understanding threat capabilities in cyberspace, senior leaders must also understand specific vulnerabilities within cyberspace.[5] This has typically been a challenge for senior leaders to understand because of the technical and often esoteric nature of cyber vulnerabilities. Additionally, cyber operators are not effective in translating a risk imposed by cyber vulnerabilities as a risk to the commander's mission. Finally, senior leaders must understand that cyber risks are not completely mitigated just because the organization has implemented the latest software patch.[6] Therefore, cyber operators must present alternative at the strategic, operational, and tactical levels that mitigate risk by addressing the threat and vulnerability collectively.

4. Since there is often a gap between a cyber-operator's explanation and a senior leader's understanding, decisions about cyber security do not always include mission assurance requirements.[7] For example, during the invasion of Iraq in 2003, a Naval Communications element decided to interrupt extremely high frequency (EHF) satellite service for routine maintenance during the same period that the Navy command center in Bahrain was attempting to transmit targeting data to its Tomahawk land attack missiles for a strike against Saddam Hussein at Dora Farms. The interruption reduced the launch capability to 39 of the planned 45 missiles, with several missiles arriving minutes later than planned.[8] While the overall impact of this scenario was relatively benign, it highlights the requirement for senior leaders to understand the impact of cyberspace decisions to their mission assurance. Commanders should insist and recognize that such decisions should not be the sole purview of cyber operators.

5. However, conducting even the most basic cyber defense tasks, such as applying software patches, configuring network components, and configuring network defense appliances is mostly reactive instead of proactive. The sheer volume of workstations, servers, and other devices, coupled with the frequency at which patches and code updates are released ensures that the Army will not be able to keep every system fully patched. Additionally, current methods for identifying vulnerabilities, developing fixes, and patching systems will virtually guarantee are not sufficient to illuminate the presence of zero-day vulnerabilities.[9] The current approach will most assuredly keep the U.S. Army in a reactive posture with respect to keeping LWN systems updated. My personal observations indicate the same results extend to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These methods still require the detection of an adversary already in the network.

6. In response to these challenges, the U.S. Army can adopt a risk management framework focused on cyberspace, but adapted from other risk management frameworks used within the land domain.

RECOMMENDATION

1. Army Operations within cyber's contested space requires the same level of risk management used in other contested domains. Most risk management frameworks use a variant of the Army's

Composite Risk Management (CRM) framework[10] or even Boyd's OODA loop.[11] Despite the existence of a higher level framework, the Army should consider a cyber-risk management framework that includes an assessment of threat capabilities, adversary intent, how LWN vulnerabilities affect the mission, and a means to develop and act on cyber countermeasures that are proactive. The framework described in this paper integrates the OODA loop philosophy with a risk assessment equation that accounts for threats, vulnerabilities, assets, and countermeasures.

2. Starting with the Observation and Orientation portions of the OODA loop[12], cyber operators must first assess the threat in terms of adversary capabilities and their willingness to execute them within cyberspace. Intelligence specialists must make a determination about an adversary's Knowledge, Skills, and Abilities (KSA) within cyberspace as well as their access to friendly networks. Additionally, cyber operators must determine if an adversary's action can be directed specifically at friendly networks and the possible effects beyond intended targets. Similarly, intelligence specialists must also determine if adversary actions against other networks will have indirect effects to friendly networks. Maintaining an accurate common operational picture of both adversary and friendly information systems will continue to be a challenge for the Intelligence Community[13], but is a necessary requirement for effective cyber operations. Aside from an adversary's actions, cyber operators must also consider governance structures, mission processes, technical architectures, facilities, equipment, supply chain activities, external service providers, and the environment in their assessment of the threat.[14]

3. Continuing with Boyd's Observation of and Orientation to the environment, cyber operators must also assess the vulnerabilities present within their cyber operational space. Vulnerabilities can exist anywhere, but are generally classified as either a design flaw or inherent vulnerability. Since cyberspace is a man-made domain, vulnerabilities can also materialize from almost anywhere in the system. The CSL Study names vulnerabilities arising from hardware, software, and users as key information senior leaders need to know about cyberspace.[15] However, a good vulnerability assessment should go beyond these three areas. As with the threat assessment, cyber operators should consider governance structures, mission processes, technical architectures, facilities, equipment, supply chain activities, external service providers, and the environment in their vulnerability assessment.[16] Combining the threat with vulnerabilities provides a partial picture of the cyber risk present on any particular network.

4. In order to gain a complete picture of the cyber risk, cyber operators must combine threats and vulnerabilities with mission assurance assets that require protection. The Department of Defense (DOD) assigns a Mission Assurance Category (MAC) to information systems. The MAC level reflects the importance of the information relative to the achievement of DOD goals and objectives with respect to confidentiality, integrity, and availability, and in particular the warfighters' mission.[17] However, these definitions may not provide sufficient fidelity for cyber operators to prioritize mission assets for a commander would, especially given the range of DOD missions the Global Information Grid supports.[18] A 2011 study conducted for the Naval Research Laboratory (NRL) developed an approach to identify factors that contribute to ascertain the criticality of an asset and determined how to combine them in a meaningful way to determine asset criticality.[19] They categorized the factors into three categories (1) external, (2) static, and (3) value-sensitive based on the way they affect different aspects of criticality and how to measure them.[19] In a separate study conducted for the Air Force Research Lab (AFRL),

researchers proposed a method to automate the mapping of Cyber Assets to Missions and Users (Camus). They demonstrated how commonly available data sources can be rapidly collected, correlated, and fused to automatically map cyber assets to the users who depend on them, to the missions they support, and to the services they provide.[20] Regardless of the method, the end result should be a prioritization of mission assurance assets that depend on cyberspace. With a prioritization schema, cyber operators can align threat and vulnerability analyses with mission assurance assets the commander is most concerned with. Additionally, using the previously mentioned approaches,[21] cyber operators can clearly articulate the link between recommended countermeasures and mission assets to commanders.

5. In the Decision and Action portions of Boyd's OODA loop,[22] cyber operators should combine the analysis of the threat, vulnerabilities, and critical assets to develop specific proactive and reactive countermeasures that can negate threat actions and reduce vulnerabilities. A good discussion of countermeasures will include a strategy and set of actions a commander can understand and has the authority to execute in order to protect critical mission assets.[23] The strategy can be expressed in terms of an organizational campaign plan through a discussion of ends, ways, and means. Only then can the commander make a more informed decision about accepting, avoiding, mitigating, sharing, or transferring the risk.[24] When the commander is seeking to mitigate, share, or transfer the risk, countermeasures can be expressed in terms of actions that can be executed at the strategic (policy), operational (process), and tactical (action) levels. This should also lead to a discussion about trade-offs and constraints of each countermeasure with respect to the impact on mission operations. Reactive countermeasures should include appropriate decision levels that can speed response times and potentially stop an attack before it becomes worse. This base of knowledge built on an understandable analytical method and response strategy should provide leadership with the necessary flexibility to balance cybersecurity against mission requirements.

COUNTERARGUMENT

1. In his remarks to the HASC in 2012, LTG Hernandez cited that ARCYBER has blocked more than 400,000 attempts to gain unauthorized access, 4,000 known malicious websites, and 400 email phishing campaigns. Additionally, the Army's Web Risk Assessment Team has scanned over 10,000 documents accessible through Army web pages in search of cyber threats. This activity resulted in reducing the Army's cross domain violations by 50 percent.[25] While the Army is currently (and has been) conducting effective actions against the cyber threat, there still exists a gap between senior leaders and cyber professionals thorough understanding of the relationship between cyber risks and the organizational mission. This gap is not unique to the military. A 2012 survey conducted by Carnegie Mellon's CyLab discovered that the private sector suffers from similar challenges. They concluded that even though there is an emphasis on risk management in general, executives do not clearly understand the linkage between information technology (IT) risks and business operations.[26]

2. Within the U.S. Army, the CSL Cyber Operations Workshop identified the need for better senior leader education of cyberspace issues and the need to provide them with enough knowledge to understand basic definitions and concepts in order to make appropriate decisions when necessary. The CSL Cyber Operations Workshop members also agreed that effective cyberspace defense revolves around risk management.[27] Therefore, a gap still exists between

Army senior leaders' understanding of cyber risk that could be partially filled with an effective risk-management framework.

CONCLUSION

To effectively communicate cyber risk to Army commanders, cyber professionals must move away from a primarily technical view of protecting cyberspace and move towards a framework that effectively links cyber threats to their potential effect against military mission readiness. The risk-management framework described in this paper accounts for the ability and intent of the threat to act, the network vulnerabilities they can exploit, and the mission assets they wish to affect. This risk management framework enables cyber professionals to develop a range of countermeasures that are effective against the threat. Furthermore, countermeasures can be presented in understandable terms relevant to mission commanders ready for execution.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. TRADOC Pam 525-5-600, *US Army's CONOPS LandWarNet 2015*, ii.
2. House, Presentation to the Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, Digital Warriors: Improving Military Capabilities for Cyber Operations on 25 July 2012, 112th Cong., 2nd sess., 2012, 3.
3. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 11.
4. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 11.
5. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 11.
6. Leitzel, "Cyber Ricochet", p. 2.
7. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 2-3.
8. Gordon, Cobra II, p. 201.
9. Leitzel, "Cyber Ricochet", p. 2.
10. FM 5-19, Composite Risk Management, p. 1-3.
11. Hammonds, "The Strategy of the Fighter Pilot."
12. Hammonds, "The Strategy of the Fighter Pilot."
13. W. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 12.
14. US Department of Energy, Electricity Subsector Cybersecurity Risk Management Process. p. 10.
15. Hammonds, "The Strategy of the Fighter Pilot."
16. W. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 11.
17. US Department of Energy, Electricity Subsector Cybersecurity Risk Management Process. p. 10.
18. DOD DIR 8500.01E, Information Assurance. p. 4.
19. Kim, Determining Asset Criticality for Cyber Defense, p. 3.

20. Kopylec, CAMUS: Automatically Mapping Cyber Assets to Missions and Users, p. 3.
21. Kopylec, CAMUS: Automatically Mapping Cyber Assets to Missions and Users, p. 3.
22. Hammonds, "The Strategy of the Fighter Pilot."
23. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 14-15.
24. US Department of Energy, Electricity Subsector Cybersecurity Risk Management Process. p. 10.
25. House, Presentation to the Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, Digital Warriors: Improving Military Capabilities for Cyber Operations on 25 July 2012, 112th Cong., 2nd sess., 2012, 4.
26. Westby, Governance of Enterprise Security: Cy Lab 2012 Report, p. 5.
27. Waddell, CSL Study 1-11, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace. p. 14-15.

BIBLIOGRAPHY

FM 5-19 (100-14). *Army Field Manual, Composite Risk Management,* July 2006.

TRADOC Pamphlet 525-5-600. *The United States Army's Concept of Operations: LandWarNet 2015,* 11 February 2008.

DODD 8500.01E. *Information Assurance (IA),* 24 October 2002.

Gordon, Michael R., and General Bernard E. Trainor. *Cobra II: The Inside Story of the Invasion and Occupation of Iraq.* New York, NY: Vintage Books, 2007.

Hammonds, Keith H. The Strategy of the Fighter Pilot. June 2002. http://www.fastcompany.com/44983/strategy-fighter-pilot (accessed 15 October 2013).

Kim, Anya and Myong H. Kang. Determining Asset Criticality for Cyber Defense. Washington, DC: Naval Research Laboratory, 23 September 2011.

Goodall, John R., Anita D'Amico, and Jason K. Kopylec. "CAMUS: Automatically Mapping Cyber Assets to Missions and Users." *Proceedings of the 2009 Military Communications* Conference (18-21 October 2009): 1-7. doi:10.1109/MILCOM.2009.5380096

Leitzel, Benjamin. "Cyber Ricochet: Risk Management and Cyberspace Operations." *Center for Strategic Leadership Issue Paper* 2, No. 12 (July 2012): 1-5. http://www.csl.army.mil/usacsl/publications/IP2-2-CyberRicochet.pdf (accessed 16 October 2013).

U.S. Department of Energy. *Electricity Subsector Cybersecurity: Risk Management Process* (May 2012): 1-86. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf (accessed 16 October 2013).

House Committee on Armed Services, *Digital Warriors: Improving Military Capabilities for Cyber Operation, Hearings before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services,* 112th Cong., 2012.

Waddell, William, David Smith, James Shufelt, and Jeffrey Caton. "*Cyberspace Operations. What Senior Leaders Need to Know about Cyberspace.*" Center for Strategic Leadership Study 1-11 (United States Army War College: Carlisle, PA, March 2011), 1-35.

Westby, Jody R., "How Boards & Senior Executives are Managing Cyber Risks." *Governance of Enterprise Security: CyLab 2012 Report,* (Carnegie Mellon University: Pittsburgh, PA, May 2012).

The Modern Application of Sun Tzu's Art of War: Improving Application to Cyber Power
Major Frederic W. Lunas, U.S. Air Force (AFIT)

ABSTRACT

Contemporary western cyber leaders fail to apply the lessons that whoever is first in the field and awaits the enemy will be fresh, not to allow the enemy's will to be imposed on you, and to make one's position unassailable, outlined in Sun Tzu's Art of War, despite research supporting the relevance of Sun Tzu's work to the modern cyber arena. Mazanec (2009) highlights its relevance, comparing asymmetric warfare to his stratagems to overcome superior with inferior forces. More specifically, Sun Tzu's relevance in the cyber arena has also been discussed by Brzozowski (2005), Geers (2009), Miller (2001), Owens (2009), and Shan (2009). Such research focused on specific lessons from Sun Tzu's The Art of War and related them to cyber. Despite ongoing research and an identified need, applying these repeatedly supported tactics to cyber has been problematic; through inflexible thinking (Brzozowski, 2005), being only prepared to deal with "conventional" threats (Detica, 2008), because cyber changes too quickly (Geers, 2009), and poor organization for managing cyber capabilities (Owens, 2009), when a flatter, broader, adaptive structure is needed (Shan, 2009). This paper will discuss how the U.S. has failed to apply Sun Tzu's lessons properly in the cyber arena, and will recommend ways to correct this.

DESCRIPTION OF ISSUE

Contemporary western cyber leaders could benefit from better application of the lessons that whoever is first in the field and awaits the enemy will be fresh, not to allow the enemy's will to be imposed on you, and to make one's position unassailable, outlined in Sun Tzu's Art of War, to the cyber arena. Sun Tzu is very much relevant today. For example, the Xavier Leadership Center's director cites that Sun Tzu's teachings have equal relevance in the business world (Brzozowski, 2005). This relevance also applies in the military arena. The U.S. military recognizes the need for cyber capabilities and their increasing importance to attain our goals. Lt Gen Basla, emphasizing cyberspace is an area so important to our nation and our nation's defense (Basla, 2011). Sun Tzu's philosophies on warfare are also very much relevant in today's cyber arena. Sun Tzu's philosophies are reflected in the titles of recent white papers Sun Tzu and the Art of War: A new chapter on cyber-security, What ancient military tactics can teach us about new threats (Lord et al, 2009), and Military principles of Chinese origin to improve competitiveness (Shan et al, 2009). Though battles fought are different, these philosophies can aid when setting up company security (Miller, 2001). Specifically, Sun Tzu has lessons that apply to the quickly growing Cyber field. For example, Detica (2008) discusses how. "Sun Tzu provides a useful … framework … for … management of cyber war" (Geers, 2009).

1. Sun Tzu offered many lessons that could benefit the U.S. in the cyber arena. For example, Sun Tzu states that whoever is first in the field and awaits the enemy will be fresh; whoever is second will arrive exhausted (Griffith and Liddell Hart, 1963). However, the U.S. failed to recognize the relevance of this advice. Sun Tzu' s advice could have been better followed by the U.S. if we had emphasized getting our forces onto the "cyber battlefield" sooner. Yet the U.S. has not always been effective at getting cyber forces onto the battlefield first. For example, as early as 2003, the Chinese People's Liberation Army (PLA) had already organized its first cyber warfare units (Mazanec, 2009). It was not until 2008 that the Comprehensive National Cybersecurity Initiative was adopted as national policy (Owens et al., 2009). In light of these developments, the U.S. has now identified the need for cyber organization. However, I assert

that more must be done to apply Sun Tzu's lesson that whoever is first on the field and awaits the enemy, will be fresh (Griffith and Liddell Hart, 1963).

Several recent articles have offered broadly differing reasons that the U.S. is not effectively following this advice. For example, Detica (2008) states that most organizations are only prepared to deal with "conventional" cyber threats such as viruses or denial-of-service attacks, but not the highly-variable threats that they increasingly face. This makes these organizations less fresh on the cyber battlefield. Therefore, the U.S. still has work to do to reach the level of our competitors.

2. In addition to being first on the battlefield, Sun Tzu's advice that the clever combatant imposes his will on the enemy, but does not allow the enemy's will to be imposed on him (Griffith and Liddell Hart, 1963) could also be beneficial; for example, as it applies to current military tactics, techniques, and procedures for reacting to a cyber-attack. However, this advice has not always been followed. In my personal experience as Wing Information Assurance Officer in 2001, when faced with cyber-attack, our procedure was to unplug affected system(s). This effectively bent us to the will of our attacker; thus, again failing to follow Sun Tzu's advice.

3. Finally, Sun Tzu's lesson to make one's position unassailable (Griffith and Liddell Hart, 1963) is also beneficial advice to follow. Many U.S. systems are vulnerable to attack. For example, industrial control systems have been left wide open to cyber-attack (DHS, 2009). Improved cyber defensive capabilities are needed because, as confirmed by an October 2009 DHS report, industrial control systems, not only traditional information systems, due to evolving links to information systems, are coming increasingly under attack (DHS, 2009). In light of these facts, our position on the "cyber battlefield" is clearly assailable, again clearly contrary to Sun Tzu's advice.

RECOMMENDATION

1. In order for the U.S. to correct the issue where we failed to follow Sun Tzu's recommendation to reach the battlefield first in the cyber domain, I recommend that we accelerate our efforts in new areas, work together with our allies, and tap the resources of our best and brightest young people. First, accelerate our efforts in new areas, such as Internet Protocol Six (IPv6). This allows us to surpass our adversaries rather than being second on the battlefield. This is confirmed by Bernstein (2009) who stated that almost all recognize the need to adopt strategies to support success in this new electronic theatre of operations (Bernstein, 2009). Second, It makes sense to create a unified cyber posture throughout allied governments and industrial bases (Mazanek, 2009). Finally, our military can tap the resources or our young innovators via education, by teaching Sun Tzu's important lesson about arriving on the field first in the modern USAF School House and looking to our young airmen to innovate ways we can move ahead, perhaps in areas where our competitors have yet to go. Once taught in a schoolhouse, the resulting ideas should be collected via venues such as the Air Force Innovative Development through Employee Awareness (IDEA) program, and any viable innovations should be applied to cyber operations to more effectively accelerate our military towards an advantage in cyberspace.

2. In addition to reaching the "cyber battlefield" first, it is important to prevent our adversaries' wills from being imposed on us. I recommend that we can achieve this by continuing and expanding our doctrinal tactic of "fighting through the attack", instead of shutting off or unplugging, in conjunction with deterring adversaries from attacking in the first place. I believe the tactic of operating during a cyber-attack will become more viable as our cyber capabilities develop. In doing so, the added challenge of operations during an attack may even accelerate development of these same cyber capabilities and the skill sets of our cyber operators. In support of my recommendations, a June 2009 Center for a new American Security Journal article calls for the U.S. government to increase economic, political, and military costs for cyber attackers while defending against them more effectively by clarifying legal authorities related to military and intelligence cyber operations, improving cyber defenses, sustaining America's offensive military advantage in cyberspace, implementing a cross domain prevention strategy, ensuring that the U.S. military can operate in a command and control environment degraded by cyber-attacks, and tapping into the National Guard and Reserves for high-tech cyber skills (Lord et al, 2009). This is a tall order, but until the U.S. Government has heeded all the advice cited in the article by USAF Lt. Gen Lord (2009), I firmly believe we will continue to fail to properly apply Sun Tzu's lesson to prevent an adversary from bending us to their will in the Cyber Domain.

3. Finally, in addition to being first on the battlefield and preventing an adversary from bending us to their will, Sun Tzu advises us to make our position unassailable. In response to this philosophy, my recommendation is two-fold. First, I would recommend strict discipline on commanders who allow unpatched systems, unauthorized configurations and/or non-standard implementation of hardware and software in their units. I firmly believe that if security guidance was properly followed across the board, the majority of attacks could be thwarted before they happened. Second, I would recommend that the U.S. and allied countries, especially those with whom we may have interdependent industrial control systems (e.g. Canada), enact laws requiring installed and properly configured security measures to thwart any reasonably-feasible attack. Therefore, we would have addressed Sun Tzu's concern by moving our position on the "cyber battlefield" closer to Sun Tzu's goal as unassailable.

COUNTERARGUMENT

Although I do not believe anyone would argue that improving our cyber advantage and the security of our systems is a bad idea, the idea of "fighting through the attack" when it comes to cyber could be debated. For example, one could counter that certain systems are simply too important to risk leaving them connected to the network during a cyber-attack. However, this does not consider systems that are operationally critical to preserve lives. However, one may counter the idea of shutting down or unplugging our vital systems with the argument that if you disconnect or shut them down, you have effectively removed their utility to us in any case. Again, systems that are operationally critical to preserve lives, if shut down or disconnected, would result in lives lost, (e.g., instrument landing systems at night for aircraft low on fuel, medical life support systems, etc.). Thus, we would affect a result on our own forces that was worse than allowing the adversary to bend us to their will.

REFERENCES

Basla, M. (2011, April 1). Lieutenant General Michael J. Basla, Vice Commander, Air Force Space Command, "Defending the Cyber Realm" Cyber Futures Conference, National Harbor, Maryland, Page 1, Paragraph 2.

Bernstein, J. (2009). Cyber Warfare's Threat to Critical National Infrastructure, Published April 2009 in MIS-ASIA, Page 1, Paragraph 4.

Brzozowski, L. (2005). Special Report, Sun Tzu to Toyota – the Essence of Speed-BasedCompetition, Director, Xavier Leadership Center, Page 2, Paragraph 3.

Detica (2008). GOVERNMENT | INFORMATION ASSURANCE, Sun Tzu and the Art of War: A new chapter on cyber-security, A Detica white paper, Pages 4-7. Available from: IA@detica.com.

DHS (2009). Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, Control Systems Security Program, National Cyber Security Division, U.S. Dept. of Homeland Security, October 2009, Page 1, Paragraph 2.

Geers, K. (2009, February 9). Sun Tzu and Cyber War, Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia, CCD CoE, Page 3, Paragraph 4.

GPO (2010, September 23). House Armed Services Committee (H.A.S.C.) No. 91–179 U.S. Government Printing Office, Page 3, Paragraph 5.

Graham, B. (2005, August 25). Hackers Attack via Chinese Web Sites, Washington Post. Retrieved June 18 2011 from The Washington Post. Available from: www.washingtonpost.com.

Griffith, S. & Liddell Hart, B. (1933). The Art of War, by Sun Tzu et al, London: Oxford University Press. Chapter 6, Paragraphs 1-2 and Chapter 8, Paragraph 11.

Lord, K. et al. (2009). The Center for a new American Security (CNAS) June 2009 Volume I, America's Cyber Future Security and Prosperity in the Information Age, page 8, paragraph Raise Costs for Cyber Attackers.

Mazanec, B. (2009). The Journal of International Security Affairs Spring 2009 - Number 14, article, The Art of (Cyber) War, section: Forging a U.S. Response, paragraph 4 and section: The roots of Chinese cyberwarfare, Paragraph 5. The Journal of International Security Affairs. Available from: www.securityaffairs.org.

Miller, M. (2001). Sun Tzu and the Art of (Cyber) War: Ancient Advice for Developing an

Information Security Program, Matthew K. Miller, Copyright SANS Institute, Version 1.2b, April 2, 2001, Page 2, Paragraph 1

Owens, W. et al (2009). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Research Council, William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Editors, Committee on Offensive Information Warfare Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, Copyright 2009 by the National Academy of Sciences, Page viii, Paragraph 1.

Shan, L. et al. (2009). Military principles of Chinese origin to improve competitiveness, National University of Singapore, Singapore.

Welshans, J. (2010). Historical Perspectives, ITEA Journal 2010 (31), History of Cyber Testing and Evaluation—A Voice From the Front Lines, Copyright, International Test and Evaluation Association, Page 449, Paragraph 1.

Exascale and Quantum Computing Impact on DOD Strategy
Mr. (GS-13) Lou Giannelli, U.S. Air Force (547 IS)

ABSTRACT

The current demand for advances in High Performance Computing (HPC) technology is vectoring our efforts through two different paths; the traditional progression within the scope of the original binary architecture, and the new computing paradigm based on the discovering of the behavior exhibited by sub-atomic particles, allowing us to redirect our efforts into the realm of quantum computing (QC). In the traditional binary architecture our nation has already lost the leadership in HPC at the petascale level. On the quantum computing level, however, there is no current leader in this race, but the runners are many. Attempts to recapture the leadership at the petascale level do not represent a feasible solution, since this level of HPC is no longer able to satisfy our scientific and technological demands, and consequently we need to focus our efforts on achieving HPC performance at the exascale level. Accordingly, in order to maintain scientific, technological, and military global superiority, the U.S. must establish HPC leadership both at the exascale and the QC levels.

DESCRIPTION OF ISSUE

There are great economic and strategic benefits in achieving exascale HPC, because these two factors pave the way to technological advancement and military superiority, and the U.S. is not the only runner in this race, which includes the current two leaders in petascale, Japan and China, plus the European Union, Russia, and lndia.[1] The ascendance of Asian countries to the top two leadership positions in HPC is not an anomaly, but rather the demonstration of how the epicenter of computing excellence has migrated from North America to Asia. Achieving HPC at the exascale level is intimately connected with the successful design, testing, and production of high energy devices, more efficient and powerful engines, optimized and stealthier fighting platforms, revolutionary materials, superior weaponry, and national, economic and environmental security.[2] This overall enhanced strategic progress is attainable via the use of powerful and versatile modeling and simulation (M&S) platforms operating at a superior level offered by exascale HPC with a performance rate of 10^{18} exaflops per second (Eflops/sec). The current operational petascale systems (10^{15} Pflpos/sec) are insufficient for the computational demands presented by the M&S requirements necessary to achieve the enhanced strategic technological progress essential for undisputed superiority. If successful, the attempt initiated by Oak Ridge National Laboratory (ORNL) to recapture HPC leadership at the petascale level may become an ephemeral and pyrrhic victory[3]; strategically it is more advantageous to redirect the efforts into achieving leadership at the exascale level.

In addition to the quest for superiority in HPC via the traditional binary path of exascale, we must also seek superiority by achieving operational leadership on the sub-atomic path of QC, allowing us to surpass the limitations imposed by the binary architecture, where we remain limited to only two states and a single choice between these two states. In QC we are allowed to transcend that limitation by being ushered into a cyber-realm where the computational universe is limited only by the number of quantum bits (qubits) we can employ, and we become empowered to operate simultaneously within all the multiple choices generated by the number of qubits employed by a given QC system. We are already benefiting from a reduced subset of quantum applications, especially in the critical field of cryptography, but we are not alone in these fields.

Supporting Point 1: The importance of using petascale HPC in scientific research and technological development is quite evident in the June 2011 version of the official list of the top 500 HPC systems, where Japan, China, The UK, Germany, France, and Russia are the nations with double-digit listings. Of all the 500 listed systems, 30% declared a cryptic unspecified application area, 15% dedicated to research, and 4% dedicated to defense, with the remaining 51% distributed among miscellaneous applications other than research or defense. It is not unreasonable to extrapolate that 30% into classified research and defense projects.[4] In our global and compulsory quest for fossil fuel the Chinese Feoso case attests to the strategic advantage of petascale HPC by reducing calculation time from 6 months to only 16 hours.[5] On the other hand, the modeling of the structure of an entire airplane interacting with atmospheric variables and sound waves under hypersonic conditions during mission maneuvers is an unattainable goal with the current petascale HPC systems. The solution requires an order of magnitude increase in computational capabilities as the ones provided by exascale HPC systems.[6]

Supporting Point 2: The gains already achieved from using M&S at the petascale level, allow us to project the enormous advantages of transitioning into the exascale level to overcome the current limitations at the petascale level. The computation of the radar cross section (RCS) of an entire modern fighter platform, given a fixed incident angle and a 1 GHz radar signal, remains unattainable with the present petascale systems. The introduction of exascale HPC can translate this issue into an attainable goal.[7] The technological advances achieved via the research into nanotechnology feed the progress into HPC as well, as demonstrated by the computing architecture of the Japanese HPC system K, currently number 1, delivering 10.51 Pflops/sec[8] and based on the "Venus" 45nm S.parc64-VIIIfx processor, with 22,032 four-socket blade servers fitted into 864 server racks, working with 705,024 cores on parallel computation operations, as an example of nanotechnology development assisting petascale HPC.[8] Petascale has provided engineering solutions critical to national defense, as in the case of simulation of a complete gas turbine chamber that reproduced the "combustion instability" phenomenon, leading to catastrophic engine failures in helicopters, rocket, and aircraft turbines. The transition into exascale HPC is critical to national security in aiding a design framework for producing optimized flying platforms and the corresponding advanced propulsion systems.[10]

Supporting Point 3: The traditional binary computational paradigm at the current HPC petascale level is limited to a single choice when performing calculations (e.g. opting for either a 0 state (off) or a 1 state (on)). In QC a qubit offers three choices; a 0, a 1, or both simultaneously, due to the quantum superposition behavior exhibited by subatomic particles. Therefore, while three bits (111) offer a single computational choice between 0 and 7, in the QC realm 3 qubits offer all eight computational possibilities at once.[11] DARPA's quantum network has been operational since 2003, offering an unprecedented level of security via Quantum Key Distribution (QKD) cryptography. Quantum related projects for 2012 include the production of nanowires and nanotubes in support of national defense applications, the former supporting QC and nanorobot programs, and the latter assisting the development of new materials and devices associated with missile defense programs.[12]

RECOMMENDATION

1. As a nation we should concentrate our efforts into the successful launching of a cyber-equivalent to "Apollo 11" in order to capture the leadership at the exascale HPC, since we

already lost the race to petascale HPC. This goal will allow us to reap the strategic advantages of achieving leadership at the scientific, technological, and military levels by becoming the first ones walking on the "moon" landscape of exascale HPC, and enhance our national security posture via the manifold scientific and technological achievements made possible via research and development (R&D) at the exascale level. Currently, the U.S. continues to sustain the emphasis on investments in R&D, but our emphasis on maintaining the leadership in strategic technologies is highly questionable, and the compound effect is that the lack of technological leadership increases our dependence on foreign technologies, thus placing us at risk through the supply chain threat. We should apply our efforts in regaining scientific and technological superiority in the areas that promise a greater return on investment, instead of attempting to catch up in the areas where we already conceded leadership to other nations. Asia has already captured the leadership at the petascale level. Therefore, we should invest our efforts in achieving exascale leadership, simply because exascale is the HPC paradigm that will unveil and unlock strategic technologies that remain unattainable at the present. The complex aerodynamic design breakthroughs required to maintain air superiority can only be achieved via M&S capabilities provided by HPC exascale systems. The first global power achieving exascale capabilities will also be the power projecting air superiority. We must remind ourselves that DARPA was created for the very purpose of avoiding strategic surprises detrimental to U.S. national security.[13]

2. As a nation we must regain control of the sensitive and costly R&D data that we produce but also allow to flow into the hands of our adversaries, thus facilitating the asymmetric advantage they steadily accumulate, to the detriment of our national security. Many technological and strategic discoveries lay unveiled beyond the horizon of exascale HPC, but such discoveries are intrinsically correlated and dynamically associated. A new aerodynamic advanced design and a corresponding propulsion system are only half of the equation, since the fighting platform must overcome the exigent demands occurring during mission maneuvers, while at the same time remaining capable of a higher degree of stealthness to defeat the increasingly powerful and efficient adversary's radar. The reduction of RCS under mission maneuvers is also a solution waiting for the ushering of exascale HPC systems capable of delivering the computational power currently unavailable from petascale systems. The cross- pollination between the research areas of nanotechnology and exascale computing will generate the foundation for the technological advances required to achieve technological and military superiority, with the production of new materials, advanced technology, and weaponry. The one problem that remains an open challenge is the unauthorized flow of R&D data into the hands of our adversaries, because as a nation we are still incapable of protecting the confidentiality of this critical data. The required protection for our sensitive R&D data is an attainable goal, but requires a transformation in our mindset; we must migrate from a reactive to a proactive cyber defense posture and from a centralized to a decentralized cyber defense construct. Our current reactive posture is self-defeating, and our centralized cyber defense is myopic. The democratization of cyber defense is a myth. Not all data sets are the same, and not all data sets reside in the same cyber environment. The more profound the knowledge of the particular cyber environment where sensitive data reside, the more effective and granular the cyber defense posture we can sustain. The adversary is neither more capable nor more intelligent than us; we are just more complacent than they.

3. As a nation we must earnestly seek to transcend the limitations of our current binary cyber architecture. The costs associated with maintaining this current binary cyber architecture will soon outweigh the benefits of HPC, even at the exascale level. The scientific, technological, and strategic horizons unveiled by QC represent both a path to a more efficient computational paradigm, and a path to technological leadership. More importantly for the DOD, the computational architecture of QC represents the path to military hegemony, strategic, and tactical superiority. And while at the present time we do not have an operational QC system, we can greatly profit from the use of already operational quantum technologies, namely, in the area of quantum cryptography. The QKD schema provides a superior level of security, even transcending dependency on current network infrastructures. Two photons can be entangled as a pair of qubits, namely, two particles sharing quantum state (spin orientation) as if they were one. The former remains at one location, and the latter is transported to another location; the state of the teleported qubit is changed, and this change is instantly replicated by the resident qubit, thus resulting in a successful case of quantum teleportation. Quantum teleportation over a satellite-assisted network is already under exploration, with the potential of offering not only land but sub-surface highly secure communications as well. The successful quantum teleportation of entangled photons achieved by China should serve as a rude awakening for DOD,[14] given the implications of the use of high-powered blue laser for quantum data exchange.[15] The transfer of intelligence through air, surface, and sub-surface constitute a tremendous tactical advantage, and we cannot afford to take second place, since the Chinese are not the only players in the quantum teleportation race, which includes Russia[16] and Europe[17] as well.

COUNTERARGUMENT

1. As a counterargument, it may be argued that the cost of developing operational exascale and QC systems exerts a tremendously onerous impact on our nation's budget, material, and human resources, and that the benefits of R&D on these two HPC paths may not outweigh the costs. This argument ignores the available evidence presented in this position paper, outlining two main factors. One, the race toward exascale and QC computing is already in place, and the resources have already been allocated by DOD and DoE. This is an unavoidable reality, and our nation cannot afford not to participate in it. Two, national security and military superiority demands not only that we participate in this race, but that we win it as well. The same desire that fueled our commitment to place a man on the moon should be rekindled in placing our flag on the arena of exascale and QC. The need for achieving leadership in HPC, both on the traditional binary path (exascale) and the quantum path (QC) is an uncontested issue, as attested by the U.S. government endorsement through the DOD HPC Modernization Program (HPCMP) and its five Defense Supercomputing Resource Centers (DSRC), including Air Force Research Laboratory (AFRL at WPAFB), Army Research Laboratory (ARL at Aberdeen Proving Ground, MD), Army Engineer Research and Development Center (ERDC at Vicksburg, MS), NAVY (Stennis Space Center, MS), and the Maui High Performance Computing Center (MHPCC).[18]

2. Another significant endorsement to HPC is provided by the DoE INCITE program, sustaining critical research in areas such as next-generation biofuels, nanotechnology, astrophysics, nuclear fusion energy, and aeronautical engineering, among others.[19] The only issue is the type of microprocessor architecture to employ in order to overcome the challenges of achieving petascale performance within viable parameters for power consumption and heat

dissipation, and developing faster optical interconnects and enhanced algorithms for optimized utilization of available computing processing cycles. However, the ultimate HPC is the achievement of quantum computational power, under conditions transcending the limitations of current microprocessors. Significant and promising achievements toward this goal have been recently reported by researchers at the Max Planck Institute of Quantum Optics[20] and at the University of California Santa Barbara.[21] We hope this is the prelude to capturing the leadership in HPC, both at the exascale and the QC level.

REFERENCES

1. Chris Nutall, "Supercomputing's exascale arms race," October 15, 2011, http://blogs.ft.com/fttechhub/2011/10/the-exascale-supercomputing-arms-race/?catid=677&SID=google#axzz1azNs4raE.
2. Rick Stevens and Andy White,A decadal DOE plan for providing exascale applications and technologies for DOE mission needs.
3. Dawn Levy, "Oak Ridge National Laboratory Awards Contract to Cray for 'Titan' Supercomputer," October 11, 2011, http://www.olcf.ornl.gov/2011/10/11/oak-ridge-national-laboratory-awards-contract-to-cray-for-%E2%80%98titan%E2%80%99-supercomputer/.
4. http://www.top500.org/
5. TradeKool: Global Business News, http://biznews.tradekool.com/13909/1/Race_is_on_for_new_generation_of_supercomputer.html, August 20, 2011
6. DARPA IPTO, AFRL contract number FA8650-07-C-7724, "Exascale Computing Study: Technology Challenges in Achieving Exascale Systems, September 28, 2008.
7. Ibid.
8. http://www.top500.org/lists/2011/11/press-release
9. http://www.zdnet.co.uk/news/emerging-tech/2011/06/21/inside-japans-top5000-k-computer-40093162/
10. U.S. DoE, Office of Science, "Summary Report of the Advanced Scientific Computing Advisory Committee (ASCAC), Subcommittee, Fall 2010."
11. http://www.defenseindustrydaily.com/schrodingers-contracts-us-explores-quantum-computing-03169/
12. http://www.smdc.army.mii/2008/TechCtr/Abstract2.pdf
13. http://www.darpa.mil/our_work/
14. Lin Edwards, "Quantum teleportation achieved over 16 km," http://www.physorg.com/news193551675.html, May 20, 2010
15. Matthew Luce, "China's secure communications quantum leap," http://www.atimes.com/atimes/china_business/lh26cb01.html, Aug 26, 2010
16. First International Conference on Quantum Technologies, Moscow, http://conference.icqt.org/,July 13-17, 2011

17. Greece WTM News, "German research brings us one step closer to quantum computing," http://www.wtmnews.grIsemiconductors-07/6158-German-research-brings-us-one-step-closer-to-quantum- computing.html, 22 March 2011

18. DOD High Performance Computing Modernization Program, http://www.hpcmo.hpc.mil/cms2/index.php, 20 June 2011

19. U.S. Department of Energy, "2012 INCITE Call for Proposals," https://hpc.science.doe.gov/allocations/calls/incite2012.

20. Max Planck Society, "Max Planck Society (MPG) Research News," http://www.research-in-germany.de/67310/2011-05-03-single-atom-stores-quantum-information,sourcePageId=12482.html, 5/3/11.

21. Science Daily, "Physicists Demonstrate Quantum Integrated Circuit That Implements Quantum Von Neumann Architecture," http://www.sciencedaily.com/releases/2011/09/110901155259.htm, Sep. 2, 2011

PART III: ACQUISITION

Cyber Acquisition, the Art of the Possible: Capabilities Applied to Cyberspace Offensive and Defensive Operations

Ms. Lynne M. Patrick, U.S. Air Force (90 IOS/SD)

ABSTRACT

The cyber domain must change its cultural mindset specifically in the arena of developing offensive and defensive capabilities for the warfighter. What has proven to be the most challenging aspect of capability development is the culture within cyber acquisition. The Air Force follows a traditional acquisition process that does not meet nor adhere to the zero-day or constant threats addressing the Air Force networks and the warfighters needs. The current acquisition culture is earmarked with guidelines and processes that plan for future budgeting in a 2-5 year planning cycle. This culture does not align with the 'speed of need' request for cyber capabilities in a real-time or rapid manner. Cyber development for future offensive and defensive tools/capabilities must have the ability to acquire the necessary resources whether it is Subject Matter Experts (SMEs) outside a current Air Force unit to the hardware needed to exploit the tool/capability in an agile dynamic manner. Funding must be available in an expedient manner to facilitate the development of this real-time/rapid capability to the warfighter in a matter of days, weeks or a couple of months, not 2-5 years.

DESCRIPTION OF ISSUE

1. How do you plan for a cyber threat that has not left a footprint or changes from one day to the next – the threat is always present? Gen C. Robert Kehler, Commander, Air Force Space Command (AFSPC) stated, "The security and prosperity of our nation is dependent on freedom of access to and freedom of action in cyberspace. While there are many benefits that come with this access, there are numerous inherent vulnerabilities. Threats via cyberspace pose one of the most serious national security challenges of the 21st Century."[1] Gen Kehler, began an effort in November 2009 titled "The United States Air Force Blueprint for Cyberspace" to address one of the critical concerns of the cyberspace domain; providing a framework to meet the evolving culture of Cyberspace and improving our capabilities. There have been many papers, publications and even an Air Force Directive Document 3-12 (2010) concerning cyber but, none really address the issues and concerns that threaten an agile, relentless threat to cyberspace and how we defend against it.

2. The current direction of our Cyber acquisition community uses vehicles for building tools/capabilities as defined in DODI 5000.02, December 8, 2008, to defend the network or provide support to our combatant commands and other national agencies which are outdated and archaic. The Defense Acquisition Management System is focused using terms of rapid acquisition but focus on development as, "Evolutionary acquisition is the preferred DOD strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing, up front, the need for future capability improvements. The objective is to balance needs and available capability with resources, and to put capability into the hands of the user quickly. The success of the strategy depends on phased definition of capability needs and system requirements, and the maturation of technologies that lead to disciplined development and production of systems that provide increasing capability over time."[2] Parts b and c in DODI 5000.2 are where the problem arises. The DODI is not written to respond to real-time or rapid acquisition of the threat. DODI 5000.02 states, (Part b) "Evolutionary acquisition requires collaboration among the user, tester, and developer. In this

process, a needed operational capability is met over time by developing several increments, each dependent on available mature technology. Technology development preceding initiation of an increment shall continue until the required level of maturity is achieved, and prototypes of the system or key system elements are produced. Successive Technology Development Phases may be necessary to mature technology for multiple development increments (section 803 of Public Law (P.L.) 107-314 [Reference (g)]). Part C: Each increment is a militarily useful and supportable operational capability that can be developed, produced, deployed, and sustained. Each increment will have its own set of thresholds and objective values set by the user. Block upgrades, pre-planned product improvement, and similar efforts that provide a significant increase in operational capability and meet an acquisition category threshold specified in this document shall be managed as separate increments under this Instruction."[3]

3. The Air Force is moving at a pace that makes us reactive to threats versus being proactive by not providing resources in an expedient manner to build our environment to better understand the threat along with an understanding of who we are and what we (cyber) provide to the warfighter. We may be meeting some of our needs from an offensive nature but definitely lagging on the defensive side. Gen Kehler made an effort in 2009 to move the Cyber domain into a proactive versus reactive domain recognizing that the constant, relentless threat to penetrate and/or disrupt our networks continues to thrive. Real-time, rapid tools and capabilities do not follow an evolutionary acquisition, phased approach, or through multiple development increments. Many of the tools and capabilities are needed in days, weeks and some in a few months. Some tools and capabilities are what the Cyber community calls burnable and do not require formalized testing (DT or OTE), training or fielding and may be used by the warfighter for only one tactical engagement.

RECOMMENDATION

1. To better understand the challenges faced by USAF units you need to understand the differences between real-time and rapid cyber acquisition. To complete this picture I would be remiss if I did not include foundational cyber acquisition but this is the crux of the challenges faced by real- time and rapid acquisition. The acquisition community understands foundational programs and their doctrine, training, and execution of contracts and programs are written towards that focus. In a recent Corona summit brief the pyramid depicted in figure 1is a graphical representation for producing or acquiring cyber tools and capabilities. The crux of the issue is focused on an Acquisition community that understands and follows processes directed at foundational projects, not real-time or rapid events. This has also created challenges with AFSPC Operations and Requirements element to support the units currently engaged in providing innovative, integrated offensive and defensive tool or capabilities to the warfighter at the speed of need. Not everything we innovate, develop, or field is focused on foundational sustainment. We cannot wait for a rigid, nonconforming process that does not understand nor address real-time or rapid development of defensive or offensive capabilities to the warfighter. Real-time means now, within hours, days or even a couple of months; not 2-5 years as is typical with the current process.

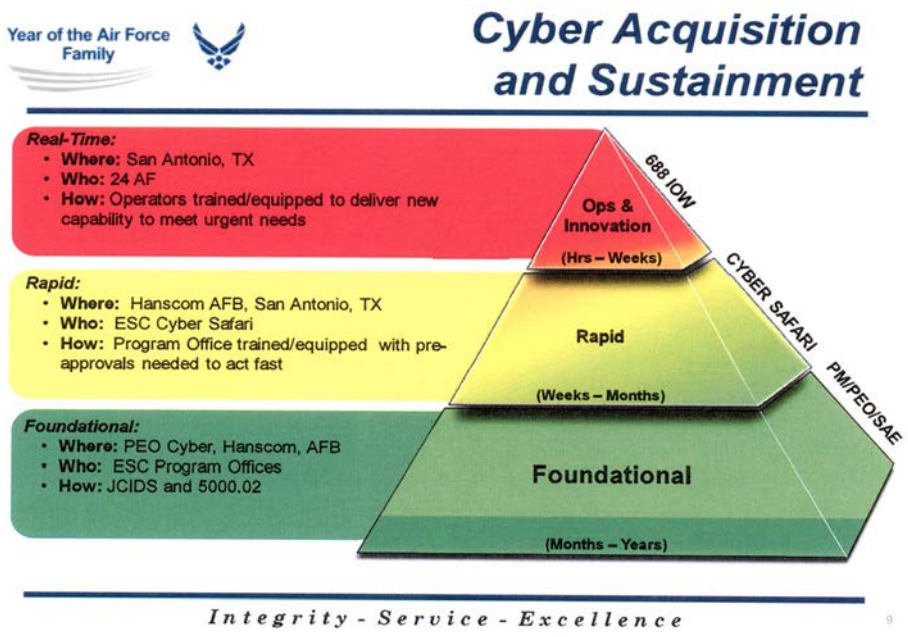

Figure 1. Cyber acquisition and sustainment

2. Through research I have found one program office, the MQ1/9 (Predator/Reaper) program that uses methods for setting aside funding to support immediate needs. Their statement of work doesn't require strict adherence to military specifications governing hardware, extensive testing programs, technical data or handbooks or other practices associated with standard equipment design or acquisition, except as otherwise noted by specific work requested coordinated through the Program Office. I recommend the engineering and developmental community follow some of their guidelines for funding, bypassing existing acquisition processes until they are mature enough to adequately address the lack of resources both in manpower and funding to the Cyber community. The Air Force must retain the lead on producing cutting edge technology, engaged with the warfighter, providing the needed tools and capabilities to defend our networks and the Air Force.

3. AFSPC over the past three years has addressed the cultural differences of Cyber and Space but not formalized the Real-time Operational and Innovation construct. Real-time Operations and Innovation do not apply to Space systems/tool/capabilities. AFI's will need to be rewritten to address the disparities between developing, testing, fielding, and sustaining a Cyber system/tool/capability versus a Space system. Not understanding the Cyber environment has proven to be detrimental also in the POM cycle over the past three years. The financial community, which includes our contracting office, must update their policies, procedures, and guidelines to work with the Cyber community producing the tool and capabilities in a real-time rapid manner. Outdated and misapplied processes and constructs to Cyber system/tool/capability procurement is still a challenge in AFSPC. Cyber cannot always tie to a valid need or requirement at least not in the current confines defined in acquisition guidelines.

4. The recommended solution for AFSPC and the Air Force Material Command (AFMC) community is to stand up of a Cyber Acquisition cell located in San Antonio, Texas. There are areas of concern and continuing disparities to what is a traditional acquisition system, tool, capability and what is Cyber. AFMC wants to formalize the rapid construct of Cyber Acquisition by manipulating the following areas:

a. Incorporate processes and tailoring of DODI 5000 series b
b. Establish dollar thresholds and contracting authorities
c. Promote competition for goods and services prior to need

AFMC also wants to formalize the foundational construct of Cyber systems/tools/capabilities by:

d. Documenting overarching processes
e. Enable integration across tiers and overall configuration control

AFMC's mission, as part of the Cyber Acquisition standup in San Antonio, Texas is to drive responsive acquisition through triage and evaluation of new or revised capabilities required in response to emerging threats based on the objectives listed below. This has the precepts of a community adjusting to the cultural change but many of their objectives and constructs are still based on an Acquisition process that does not apply to Cyber.

AFMC Objectives

- Sustain the baseline through robust integration, engineering, and testing
- Proactively engage with 3rd parties
- Facilitate agile response to changing requirements
- Promote active user involvement
- Facilitate integration, evaluation, discovery, and test
- Enable full spectrum operations

COUNTERARGUMENT

If AFMC can stand up a Cyber Acquisition Cell within the heart of the Cyber community fully integrating, understanding and grasping the concepts, innovation, real-time and rapid response to the threats via cyberspace which pose one of the most serious national security challenges of the 21st Century then we are heading down the right path. As of July 2012, the first implementation of the Cyber Acquisition construct is to be put in place at Lackland AFB in San Antonio, Texas. AFI's, directives, how we fund Cyber innovation, revamp Functional Managers, and contracting mechanisms, testing, training, fielding all need to be addressed and as General Norton Schwartz, Chief of Staff of the Air Force stated, "cyber operations reinforce and enable everything we do from administrative functions to combat operations."[4] We must have a cultural environment within the Air Force that addresses the cyberspace domain within offensive and defensive constructs of "support the warfighter." Figure 2 is a graphical representation of a proposed solution and way-ahead for communities involved in the development and acquisition of Cyber capabilities.

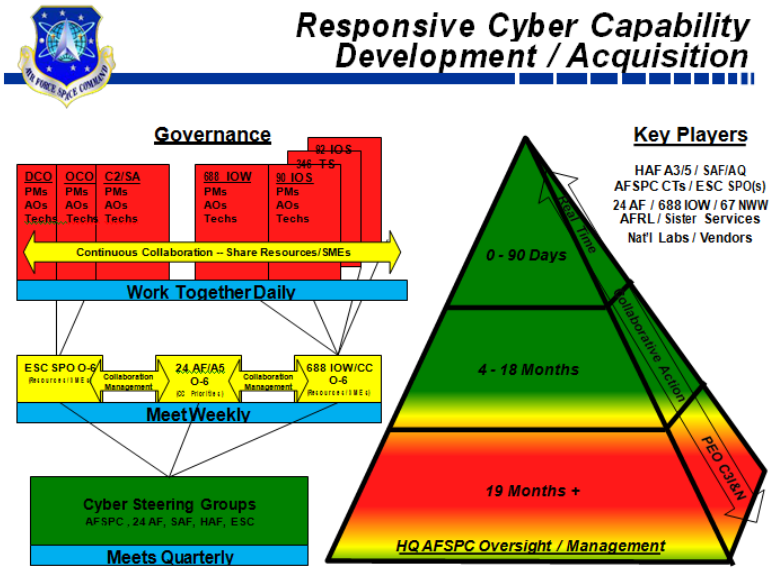

Figure 2. Responsive cyber capability, development, and acquisition

CONCLUSION

The objective is to balance needs and available capability with resources, and to put capabilities into the hands of the warfighter quickly. This is easier said than done with the current constraints the DOD is facing with manpower and funding shortages. I call this the "must haves list" for the Air Force to support the COCOM needs for real-time rapid development of defensive and/or offensive tools and capabilities:

1. Our acquisition community, to include finance and contracting, must provide agile and adaptive processes to ensure requirements are met in days, weeks, month's period of time not years. The standup of the Cyber Acquisition Cell is the right step but it has taken almost 3 years to see only the beginning of this cultural change put in motion. The acquisition, contracting and finance community will need to retrain their personnel, work closely with the operational and requirement elements within AFSPC to truly understand the phases of Cyber tool and capability development, procurement and fielding.

2. Air Force leadership must cultivate a new mindset understanding the day-to-day execution requirements needed by the AF/COCOM for Cyber components (tool and capabilities). USAF units are not being resourced to support the constant and relentless threat to the cyber domain that overall affects all of us. Many of the current resources are engaged with acquisition, contracting, and finance sections to ensure tool and capabilities are being delivered but not at the pace needed by our warfighters.

3. Though not discussed in detail in this paper, we must look at how we train to include professional military education, how we exercise and how our day-to-day operations impact the Cyber domain. What is needed to successfully acquire and meet the warfighter needs affects many of those in the Air Force. You cannot just focus on one aspect of the process. We have to get away from our stove pipe cultural communities and realize a revamping of

what is Cyber, how it is used and what is needed to ensure we put the tool and capabilities into the hands of the warfighter at the speed of need.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Kehler, The United States Air Force Blueprint for Cyberspace.
2. DODI Directive 5000.02, Reference b & c, page
3. Ibid.
4. Gen Schwartz, *Message to Airmen*

BIBLIOGRAPHY

Kehler, C. Robert (2009), The United States Air Force Blueprint for Cyberspace

Kehler, C. Robert (2010), Briefing, Cyber Update and Way Ahead

Schwartz, Norton (2009), Message to Airmen.

DOD Directive 5000.02 (Reference (b)), the guidelines of Office of Management and Budget (OMB) Circular A-11 (Reference (c)), and the various laws, policy, and regulations listed in Enclosure 1 of this issuance.

AFMC Brief (not published outside AFSPC or AFMC), Cyber Capabilities, Responsive Development and Acquisition.

Bring Your Own Device (BYOD) Vulnerabilities vs. Effectiveness

Mr. (GS-13) Patrick Abell, U.S. Air Force (USSTRATCOM)

ABSTRACT

Bring Your Own Device (BYOD)? What in the world is that? For those that don't know, it basically allows employees to bring their personally-owned devices to work and get their corporate information on them. Would that make an organization more vulnerable or more effective? Perhaps both? In today's world and fiscal restraints, we are continuously seeking out ways to try and save money where we can, keep our networks and information safe, and keep employees happy. Most people are not exactly thrilled about carrying two or more mobile devices either! It's now becoming a hot topic and the latest buzz word; BYOD. How does your organization decide if BYOD is an option for them? Money can be saved on hardware costs and monthly data plans, productivity may even go up, but at the potential expense of your organization's security; is it worth it? For your organization, this decision will have several factors that need to be taken into account and thoroughly thought out.

DESCRIPTION OF ISSUE

One issue facing the Department of Defense is also a new buzz word heard around the world; BYOD. What is BYOD? It stands for Bring Your Own Device and is defined in a few ways, all similar in fashion: employees using their own mobile devices to access their place of employment's resources such as email, contacts, calendars, network resources and information/data. Devices range from cellular phones, smart phones, laptops, notebooks, netbooks and tablets. Basically, employees are mixing or blurring the lines between work and play by using their personal device or devices at both home and work. Bring Your Own Device is becoming more widely discussed across the Department of Defense. At this time, it seems to be on a back burner but perhaps that's because of other large topics or issues that are currently on the table that take precedence over a new buzz word, keeping employees happy, or providing them with options. However, that doesn't mean that a Bring Your Own Device solution shouldn't be widely considered and tested in the Department of Defense for benefits and/or disadvantages, cost savings, increased user experience, and so on.

1. Leveraging Technology. The Department of Defense is not leveraging technology to its advantage when it comes to a Bring Your Own Device environment. Not doing so is a failure on our part.

2. Cost Savings & Cost Benefits. For all organizations or Government entities, cost benefits and cost savings are a hot topic. If there are savings to be realized, you can be guaranteed that leadership is listening.

3. Standardization. Standardization is typically a goal of any organization whether its government or commercial. Standardization is a good business practice that the Department of Defense is not following with their mobile devices or mobile device solutions.

4. Enhanced User Satisfaction & Productivity. Enhancing user satisfaction and increasing productivity is also typically a goal of any organization. The Department of Defense is making an effort in this area but could do a better job of it when it comes to mobile device options.

RECOMMENDATION

The Department of Defense needs to move forward with a Bring Your Own Device environment. Potential benefits of moving to a BYOD environment are enormous! The four categories of leveraging technology, cost benefits and cost savings, standardization, and enhanced user satisfaction and productivity would provide significant benefits to the DOD. In the author's opinion, the potential number of benefits far exceeds the potential negatives or concerns. Perhaps the weight of the negatives is the concern or it may just be the negative perceptions associated with security in the DOD and putting up a road block so that they do not or cannot move forward with newer technologies or ideas.

1. Leveraging technology is using industry's best practices, device discovery, managing multiple platforms, securing remote communications, enhanced user self-service, and identity control. All of these items can typically be achieved by implementing the right service or technology. As with any large project this should be heavily researched and tested to ensure you implement what is best for your needs.

2. Cost benefits and savings come from several different factors that include device costs, lifecycle replacement, monthly plan savings, licensing, warranty, operations and maintenance (O&M), reductions in manning or reutilization savings. Reductions in manning come from the reduction of purchasing requirements, billing and invoicing specialists, asset management, and various others.

3. Standardization is a large ongoing issue within the DOD from the author's point of view. Whether it is technology, vendors, service plans, and the list goes on. In the case of BYOD technologies it is very dependent on hardware, infrastructure and people and processes. Thankfully the DOD is making a large attempt to standardize their infrastructure and move towards a shared services environment and a cloud type technology.[1] This action will definitely help while trying to standardize our environment and improve communications and collaboration across all entities of the government.

4. Increased employee satisfaction and productivity is also a benefit of a BYOD environment. While it may seem small or without effort, many will disagree. Bringing intelligent and hardworking individuals to the government or even retaining them can be a struggle. Any advantage or option the DOD has, they should leverage it to the best of their ability. Lastly, federal workers are here to serve and protect. That includes watching out for tax dollars that all citizens pay and the services that are provided for them. A staggering 69% of surveyed government employees believe increasing mobility will enhance services to the citizens of the United States of America.[2]

COUNTERARGUMENT

1. Some counterarguments, opposing views or negative perceptions for BYOD environments are that it's too hard, it's not secure, there's too much risk to our network, and finally user privacy concerns. It has been stated by some security experts and researchers that moving to a BYOD environment is too hard.[3] Is that even a real answer? A second grade teacher wouldn't accept that answer from a student and neither should America's tax payers or those in the government workforce. Many organizations from industry and government have made the

switch to a BYOD environment. The DOD needs to embrace and leverage this technology as well and perhaps learn from a few of the organizations which include Napa County, DLA Piper, Qantas, IBM, DELL, Halliburton, Clorox, Standard Chartered, AstraZeneca Plc, Thames River Capital in the United Kingdom, The Pentagon, the Office of Immigration and Customs, The White House, and the office of Veterans Affairs.[4] The excuse of it's too much risk to our network shouldn't even be an allowed excuse. Really? Change the way networks are utilized. Let's not forget we are on an unclassified network. If it's sensitive, raise it to the next classification. Collapse a network and save even more money; MUCH more! Perhaps just consider limiting remotely accessible information. Limit it to non-sensitive information or a special level of device sophistication.

2. User privacy issues are also a concern. Users do not welcome their personal information being explored, captured or recorded. However, it seems that users may have to give up a little privacy for the convenience and desire of a BYOD environment. Is it worth it to you? It surely is to the author of this paper. Thankfully, there are mitigating factors to all of the potential concerns and counterarguments. Tactics, techniques and procedures should be put in place for regulating a BYOD environment. Agreements such as: devices may not be explored; personal email traffic may not be monitored or captured, and web browsing may not be monitored. Only government data and email should be explored and the actual exploration may not have to take place on the device, should it be on the device it will be in a secured container. Since the government email would funnel through its normal network channels/secure devices it could be explored just as it is now; no invasion may even be required. Different levels of accesses could also be offered. Some examples would: Option one: email/calendar/contacts. Option two: Shared services or SharePoint. Option one requires less from the users and would be less of a personal invasion. Option 2 would require additional security precautions, perhaps a Virtual Private Network (VPN) type solution. Author Dave Michaels recognizes the potential cost and security issues with so many device options on the market and foresees a type of "tiered support system, where some devices are fully supported, and others are tolerated."[3] Passwords and personal identification numbers could be required for all devices and data at rest with encryption could be required for the shared services/data. Patching and firmware updates would be verified and required upon accessing the network; updates would be mandatory on all devices and would be pushed from the server or updated manually by users. If devices are not 100% patched and up to date; no email or shared services access would be allowed. Remote locking and wiping capabilities would also be mandatory for users. Users would have to sign an agreement, much like today, stating they agree to all updates/patches, remote locking and remote wipe options to be placed on their device as a precaution. If a classified message incident (CMI) occurred, the device would have to be wiped and formatted just as Blackberry devices are today. Anti-Virus and Malware protection may also be a requirement based on the type of device and the capabilities required.

CONCLUSION

1. In conclusion, the author has shown that a BYOD solution can make your organization more effective, increase productivity, save money, keep our networks and information safe, and make employees happy. There are huge potential savings with BYOD. One easy example is from United States Strategic Command (USSTRATCOM). All numbers and information listed within this example are from the author's previous job and positions held.

USSTRATCOM has a little over 300 users on unclassified government-owned cellular devices. The average cost per month is about $80 per device. That equates to $24,000 a month. They have no upfront device cost at this time but easily put out $25 a year per device on accessories equaling $7,500 a year. Annual maintenance fees cost about $5,000. None of this information includes overage charges on monthly plans, broken devices or various other costs. A one year savings with only this information is about $300,000 per year for a single Combatant Command (COCOM). Multiply that across all ten COCOMs to achieve a potential cost savings of approximately $3M. The savings would be higher if users at a base or camp level across all four services are included. How about adding laptops? Add in the rest of the federal sectors. There are over 2.7 million federal employees working in the United States Government according to census surveys.[5]

2. The annual cost savings would be estimated in the billions of dollars and the Government could certainly apply the savings elsewhere; perhaps the deficit, in place of DOD budget cuts, the options go on. In addition to these costs, there are other potential savings on items like manning, training, lifecycle replacements, and licensing costs to name a few. BYOD technology is not going to go away and our mobile and remote capabilities continue to grow across the U.S. population today. The DOD needs to leverage current and future technology to do more with less, take advantage of the cost benefits, cost savings, standardize our environment to the best of their ability, and allow for enhanced user satisfaction and employee productivity. A survey of 9,513 U.S. adults, conducted online from June to August 2012, found that 22% of U.S. adults own a tablet, twice the number from a year earlier, while 44% of U.S. adults have smart phones, up from 35% in May 2011.[6] With the DOD moving towards a Joint Information Environment (JIE), we need to open our eyes and do it holistically and look at our entire environment, not just bits and pieces.[1] From the author's experience, pilot tests and project involvement, Unified Communications (UC) is another large push by our industry and Government. Again, the DOD needs to look at it holistically, not in the normal stovepipe fashion. As stated by our own current President "I want us to ask ourselves every day, how are we using technology to make a real difference in people's lives."[7]

3. Mission drives agencies and the need to deliver better services to customers at a lower cost—whether an agency is supporting the warfighter overseas, a teacher seeking classroom resources or a family figuring out how to pay for college—is pushing every level of government to look for new solutions.[7] According to a recent survey completed by the SysAdmin, Audit, Network and Security (SANS) Institute a large majority of organizations surveyed allow employees to use their own devices despite not being comfortable with the effectiveness and comprehensiveness of their policies to protect their resources being accessed by these devices. This means that organizations need to continue to provide support and guidance concerning the most secure ways to use and control mobile devices.[8] Let's go DOD, do the right thing!

REFERENCES

Teresa M Takai. "Memorandum from the Chief Information Officer of the Department of Defense" July 2012. http://dodcio.defense.gov/Portals/0/Documents/DOD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf.

Julie Anderson. “BYOD: Government Workers Could Give Up Privacy in Exchange for Convenience” May 24, 2012. http://safegov.org/2012/5/24/byod-government-workers-could-give-up-privacy-in-exchange-for-convenience

Dave Michaels, “BYOD: Here to Stay or Doomed?”http://www.ucstrategies.com/unified-communications-newsroom/byod-here-to-stay-or-doomed.aspx

Gryphn, “Government, Industry, and Enterprise Switch from Blackberry to BYOD,” November 2, 2012, http://gryphn.co/2012/11/02/government-enterprise-switch-from-blackberry-to-byod/

Office of Management and Budget, The Washington Post - Oct. 1, 2010.http://www.washingtonpost.com/wp-dyn/content/graphic/2010/09/30/GR2010093007473.html

Matt Hamblen. “Half of US adults own a smart phone or tablet, Pew survey says.” Computerworld. http://m.computerworld.com/s/article/9231902/Half_of_U.S._adults_own_a_smartphone_or_tabl et_Pew_survey_says

Digital Government, Building a 21st Century Platform to Better Serve the American People.http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital- government.html (accessed December 1, 2012)

Kevin Johnson. “SANS Mobility/BYOD Security Survey.” A SANS White Paper. http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf

The Importance of Cyber Design: The Inescapable Connection between the User Experience and Mission Assurance

Major Benjamin Dean, U.S. Air Force (National Defense University)

ABSTRACT

In broad terms, for over twenty years the Air Force has struggled in its effort to both define its role and operate efficiently within the cyber domain. Through directives, policies, and mandates, the USAF directed all of its users—*regardless of their mission responsibilities*--become "cyber operators". Airmen of every USAF Specialty Code (AFSC), civilians at every level, and contractors from every project have been directed to change their internal processes to conform to the needs of the network. Sharing, storing, and securing information are to be done under strict guidelines with help through mandatory training for all. Unlike other domains which have defined operators and designated areas of responsibility, our community has allowed the cyber domain to expand through "mission creep"—engulfing USAF users and mandating all become cyber-savvy to perform their job, regardless of mission. Not only has a change of behavior been propagated to correspond to the new demands required by the cyber domain, but the USAF has also opened up the cyber battlespace to non-cyber professionals. For those non-cyber operators, the cyber domain should be integral to their mission areas, but by operating "behind the scenes" to enhance their objectives, essential to their operations yet not complicating or forcing change on them. This can be done by introducing a new priority on "design". Designing an IT asset with a singular focus on creating a superior user experience will strengthen cyber's hand in effecting real enhancement to the mission assurance of the overall USAF mission. By infusing the concept of user-focused design into further development of the cyber domain, the AF can greatly optimize mission assurance. The cyber domain should have defined operators (17D Cyber Operators) and allow other skill-sets to enjoy an intuitive, user-focused design interface. This paper will show an operational need to create a more customer-centric, user- experience and illustrate the mission importance of quality cyber design for both cyber operators and non-cyber users.

DESCRIPTION OF ISSUE

1. The Air Force has a problem. This problem is so large; it spans all mission areas, crosses into all career fields, and it continues to grow. The connected world of networked information systems has evolved into a new operational battlespace. Today, an adversary can conduct offensive and reconnaissance missions in stealth without using traditional kinetic weapons or even leaving their country. This new realm, the cyber domain, is here to stay—joining the other domains of air, land, sea, and space. But unlike these other domains, the cyber domain is man-made and not comprised of a conventional natural area. It resides inside a fabricated, artificial domain we refer to as "cyberspace." Spread across millions of networked information technology (IT) appliances and hundreds of thousands of networked servers, it is software (a series of 1's and 0's) streaming across the entire planet. From ordinary computers in office buildings and homes, to satellites and personal mobile devices, the reach of the cyber domain is limitless. Cyberspace touches everything that is connected directly and indirectly with IT-related resources. In terms of USAF mission assurance and risk mitigation, this reveals a sobering truth, *everything is vulnerable*.[1] Every Technical Order (T.O.) on flight line laptops, every mission database in operations, and every x-ray image in hospitals are stored on networked computers. In the beginning, the USAF communications community put in place a network with little emphasis on user-focused design. And in a rush to protect our networked

infrastructure, the USAF asked both communications and non-communications personnel to conduct mandatory training, compelling both to adhere to strict procedures when logging on to the network. Over time, both of these shortcomings grew from an inconvenience to a disruption, and in some cases mission failure. Moreover, as the cyber domain matures into the future, if nothing changes, we will witness the continued escalation of mission failures due to ineffective management of the cyber domain. As the USAF communication community becomes more of a "Cyber Community," (taking steps to professionalize the USAF Network (AFNet)), we will witness continued network shortcomings as we impose more and more changes to the network (affecting their internal mission processes) to satisfy our cyber requirements. We do this because we in the cyber community are ultimately responsible for the health and functionality of the cyber domain. But as we move to the beat of our own drum, we continue to neglect the wants and needs of users as we proceed. Instead of optimizing the use of the cyber domain to enhance the customer's mission assurance, we use the cyber domain to force behavior modification on everyone in the USAF and in the process, continue to impede overall mission assurance. There is a direct correlation between the effort we make in designing AFNet (to maximize the user experience) and the contribution cyber provides to the overall USAF mission.

2. In its blueprint on cyberspace, the USAF acknowledges that "cyberspace touches practically everything, everyone, every day."[2].. It is due to this realization that cyberspace, and the activities of the cyber community, will have an effect on every USAF mission responsibility. Unfortunately, in our haste to react to the new reality of an interconnected world, the USAF built its IT networks in the absence of a user-focused design, forcing all users to comply first with the needs of the cyber community. Instead of engineering the AFNet around customer needs, we put in place a network and instructed customers to adapt to the network. Also stated in the Blueprint is the idea that, "every USAF Airman, government civilian, and contract partner must become a cyber-defender."[3] The USAF expects each user to become cyber-savvy, regardless of the level of strain on their productivity and mission accomplishment.

3. It might be difficult to underscore just how dire our situation has become. Fragmented and un-professionalized, the cyber domain is plagued by security vulnerabilities from ordinary users we allow to act as operators. For years now, the cyber community has steered non-cyber users to work "in" the cyber domain. Instead of offering them secure tools to work with to "use" the domain for support of their mission, we opened the door and provided them access to work "inside" the domain. Unlike other domains, where users simply support operators, the cyber community has classified everybody as a "cyber defender;" thus, pulling each user into our battlespace. We provide a basic level of understanding through training, then give them basically "carte blanche" access to the network, creating opportunities for unauthorized persons to manipulate computers, databases, and information as they need to create, store, retrieve, search, move, make available, delete, transfer, scan, establish permissions on files, update, upgrade, and acting as assistant IT security specialists by acting on antivirus actions to understanding and complying with USB hardware mandatory safeguards. Most of these correspond to system administrative activity, not "Operations". As useful and important as these activities are, they do not constructively contribute to mission assurance. Theoretically, tools could be created to perform a large number of these tasks. Tools designed for their

mission; designed to improve their operations posture; designed and engineered to exponentially improve the speed in which they carry out their kill chain.

4. It's not only security and accessibility that should guide us toward a more user-focused design of the AFNet. *Functionality* should play a vital role in how we support USAF mission areas. Let's look at an example to illustrate the point. It wasn't too long ago that people engaged in information sharing on the Internet mostly using email. It was simple, quick and less cumbersome than the postal service. Fast forward to today. Why did a huge majority of people migrate to texting? Chatting? Blogging? Or how about the increased use of Apple's iCloud, Facebook, or Twitter? People still have access to email, so what's the deal? Simply stated, they found *improved value* in these other forms of communication. These customers were not forced or cajoled yet millions of them *prefer* using these formats over email. Another example is have you ever been to a USAF base that mandated the use of SharePoint to share files in lieu of emailing attachments? Good luck finding many people who complied. The process is slow, arcane, and has more connectivity issues than a typical user will tolerate. So what do most users do? They simply email the attachments. It's quicker and easier. Customers value time and effort. In this case, the user-experience is perceived as being better using email than SharePoint. There are many examples where users take the easiest path to complete a task. Sometimes encrypting emails doesn't always work. PKI sometimes poses challenges when trying to encrypt. So what is the work around? The user simply doesn't encrypt. The user might warn the recipient ahead of time, but often the email with accompanying attachment gets to the recipient and both move forward with the task at hand. Again, users will get the job done following the path of least resistance. In these cases, the cyber community expelled resources to "fix" user problems without user inputs. The key to getting users onboard with cyber solutions is to increase their involvement in the initial plan to offer improved design. As professional cyber officers, we have a duty to optimize IT around the user's goals to create the best, simplest, and easiest user experience we can offer.

5. As astonishing as it sounds, the Air Force does not have cyber supremacy of our own networks. Even exempting from consideration the clandestine efforts of adversaries (both inside and outside our network), we still find ourselves woefully inept at mitigating the risk of our largest weapon systems...the collection of USAF networks. After more than two decades, the USAF cyber community still fails to provide adequate redundancy of networked systems. Efforts at Continuity of Operations (COOP) for USAF networks remain sporadic and consist of mainly rudimentary, underfunded local solutions. Additionally, inconsistent network reliability plagues our systems, introducing risk into each and every USAF mission, campaign, and sortie. The USAF allowed the sprint into the cyber domain obscure its judgment to construct a deliberate, reliable network.

6. The scope of neglect reaches far beyond network servers and backbone infrastructure. It goes all the way down to the user desktop. With a little training and some comprehension, we have forced each user to become their own mini-system administrator. Regardless of operational tempo or mission need, users must come up with their own solutions for file management. Forcing them to brainstorm their own resolutions, they procure things like DVD writers (to aid in transferring information from one system to another, often called "SneakerNets"[4]), external hard drives (for back-ups), and all sorts of Input/Output (I/O) devices

with the expectation some might be useful. When users buy IT products merely for information protection or maintenance of their data, it's a failure of cyber operations. If we were to design our network around the user, focusing our energy and skill to simplify their tasks, the user's goal would be better served and the success of that USAF mission would be further reinforced.

7. Another area of the cyber domain that could benefit enormously through a renewed focus on the user experience is secure data convergence. We maintain multiple networks at multiple security levels. The USAF created "air-gapped" stovepipes of information infrastructure, separating information based on the hardware on which it resides. These disparate networks contain voice, data, imagery, and video, creating another layer of complexity for the analyst. As protectors of information in the cyber domain, the USAF purposely separates information into these hardware enclaves. This increases the IT footprint, creating duplicate computers, networks and wiring which makes it painfully more difficult for the user to collect, consolidate, and manipulate data into intelligence. If the goal is to use the cyber domain to integrate data from all sources to come up with actionable information, why do we continue to process information based on the hardware it's on, not the content of the information? Constructing multiple platforms, in a nonlinear approach, to protect information, is a source of constant difficulty. For some users (mainly intelligence customers) this current process causes at best mission stagnation, and at worst mission failure.

RECOMMENDATION

1. As the cyber community continues to mature, Cyber Operations should proceed to aggressively train its operators to build a profession capable of executing orders to deliver the required effects of attacking, exploiting or defending a network. We should offer a level of competency second-to-none. But as for being the chief architects of the cyber domain (USAF portion), we should strive to keep cyber-related mandates off U S AF users as much as possible. Working with users, cyber operators should introduce policies, procedures, and tools designed to enhance mission areas, not levy impositions on them. By adhering to the concept of user-focused design, cyber operations can greatly optimize mission assurance. Our single most important effort should be to create a superior user experience. The easier it is for USAF users to accomplish their mission, the more we contribute to enhance mission assurance. Forbes magazine recently commented on the increased importance of design in its article *Welcome to the Era of Design*, "Design-oriented organizations invest in thinking this stuff through. They put design at the heart of their company to guide innovation and to continually improve products, service and marketing. They recognize that a great design leads to differentiation, customer loyalty and higher profits."[5] Concentrating on a user-focused design approach optimizes the use of the AFNet for users, dramatically reducing impediments brought to the table by the cyber domain.

2. One of the many responsibilities we have as cyber operators is to act as primary maintainers of the cyber domain. For one reason or another, we haven't been able to effectively leverage this domain. The solution to the bulk of our problems rests in how we shape the way in which users interact with the cyber domain through improvements in our application of user-focused design. By improving the user experience through user-requested design changes, the USAF can rid itself of many burdensome policies that impose large responsibilities on non-cyber users. In *The Art of War*, Sun Tzu discusses the five constants one

should consider prior to an engagement. The first one of these discusses the importance of having an effective policy everyone understands, "...ensure the people to be in complete accord with their ruler."[6] For years, the cyber community neglected this first tenet in *The Art of War*. Non-cyber users have maintained a love-hate relationship with cyber operators. In their need to store back-up files or their need to SneakerNet information, we tell them to fend for themselves but follow our policies. In other areas, such as changes to the ever-increasing length of passwords; authorized use of USB drives; don't use USB-drives; mandate certain training; expand 8570 training; allow A6's to authorize certain computer purchases in this command; allow other A6's to disallow the same purchases in other commands; make changes to AFWay so no one can buy previously accepted computers; and other similar disparities. The inconsistent policy changes and schizophrenic behavior provides rationale to have a lack of confidence in cyber. The solution presented here would alleviate a lot of this distrust. By shifting our focus to improved design, systems and processes will improve for the better, allowing users to concentrate more on their mission and less on complying with arcane rules forced on them by cyber operators.

3. Another solution we can provide the USAF is increased risk mitigation. With complete mission reliance on networked systems, it is increasingly apparent the USAF must change its attitude toward funding redundancy. At any time, any location, on any platform, users should be assured they have access to their information. Our job should be to ensure they get it. The haphazard way in which individual units take it upon themselves to build creative redundancy solutions on their part of the AFNet must end. Although collectively as a community we may have redundancy and COOP plans on paper, the USAF has yet to fund these mandates. Redundancy and COOP plans should encompass a single USAF plan, involving both of our Integrated Network Operations & Security Centers (INOSCs). For day-to-day usage, secretaries and Airmen on the flight line shouldn't have to ask their units to purchase back-up drives or burn CDs to conduct SneakerNet operations. It is up to the cyber operators to work with units as they come up with requirements.

4. In their 2005 report to the President of the United States Marc Benioff and Edward Lazowska raised the alarm on certain vulnerabilities, "...The [US] IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects....although current technical approaches address some of our immediate needs...fundamentally different architectures and technologies are needed so the infrastructure as a whole can become secure."[7] Safeguarding information is a chief concern for cyber operators and mission specialists alike. Users who operate in multiple security levels, must operate on multiple systems on multiple networks. This makes it difficult for the user who consolidates information pulled from multiple security platforms and analyzes the data to paint a complete and thorough operational picture. To improve on this method, the USAF should work with the users to design a network that secures information, not hardware. By encapsulating each IP packet with an encrypted, identifiable wrapper, information can be properly labeled with designated security tags, allowing information to flow across the same infrastructure, completely bypassing those systems without the proper security designation. By securing information, and not the network hardware, the USAF can finally fulfill its goal to implement "...a single, integrated network encompassing air, terrestrial, and space layers that is managed and

commanded/controlled as a single entity and that is fully compatible with a seamless DOD network."[8]

COUNTERARGUMENT

One of the primary distinctions the cyber domain has above other domains is that it's inherently manmade[9] (artificial). Advances in technology has allowed networked devices to infiltrate our lives to the point of being ubiquitous—computers, phones, handheld PDAs, automobiles, houses, television sets, fire and security alarms, irrigation systems, and even refrigerators are all networked and interconnected. There is now a battlespace that surrounds us, no matter where we are. Every Airman, civilian, and contractor has been drawn into the cyber domain. Their missions vary, but the dependence these users have on the network cannot be understated. They must all operate in the cyber realm. Now that we understand that everybody, in every mission, will operate in the cyber domain, the next focus is on *how* they operate in the domain. If our foremost concern is mission assurance, then we should look at mitigating the risk introduced by networking all USAF computers. The main risk to the network is the USAF user. Now that we have made all users, cyber and non-cyber, operators in the cyber domain, instruction, training, and formal set rules are a necessary part of conducting operations. Therefore, it's entirely proper to mandate training and direct users to follow certain rules when working inside the USAF network. All users must be knowledgeable of fundamental cyber security.

CONCLUSION

Commercial companies such as Apple, Facebook, and Twitter use design to distinguish their products and seduce their customers. In this "Era of Design," they spend millions on research to discover what users think and what they want, and—more importantly—how can we best improve our products to attract them. By creating a product or a service that fills a need, is simple to use, and maintains a measure of elegance in its design, these companies continue to find success in their mission to transform how the world uses information. There is little doubt about the inescapable connection between creating the superior user experience and mission effectiveness. By focusing our attention on finding solutions to user's tasks, we can enhance their ability to execute their missions. And by doing so, cyber operators will become an effective partner, supporting the larger USAF mission.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Quadrennial Defense Review Report, 37, para 3.
2. The United States Air Force Blueprint for Cyberspace, 2.
3. The United States Air Force Blueprint for Cyberspace, 7.
4. Ackerman, Google Drive and the End of SneakerNet, 1.
5. Swann, Welcome to the Era of Design, 1.
6. Tzu, The Art of War, 157.
7. Benioff, Cyber Security: A Crisis of Prioritization, 1.
8. The United States Air Force Blueprint for Cyberspace, 5.
9. AFDD 3-12, Cyberspace Operations, 2.

BIBLIOGRAPHY

Ackerman, Dan, Google Drive and the End of SneakerNet, Cnet.com, 22 May 2012, http://reviews.cnet.com/8301-3121_7-57437434-220/google-drive-and-the-end- of-sneakernet/

AFDD 3-12, *Cyberspace Operations*, 15 Jul 2010

Benioff, Marc and Lazowska, Edward, *Cyber Security: A Crisis of Prioritization, Report to the President*, February 2005

Gates, Robert, *Quadrennial Defense Review Report*, February 2010

Swann, Adam, *Welcome to the Era of Design*, Forbes.com, 3 May 2012, http://www.forbes.com/sites/gyro/2012/05/03/welcome-to-the-era-of-design/

Tzu, Sun, *The Art of War*, (e-Book) Translated from Chinese by Lionel Giles, 1910

USAF Blueprint, *The Air Force Blueprint for Cyberspace*, 2 November 2009

Recommendations for Open Source Development
MSgt Joseph E. Harkleroad Jr., U.S. Air Force (624th Operations Center)

ABSTRACT

The Air Force is being held back in its efforts to achieve dominance of the cyberspace domain. The platforms from which it operates are ill-suited to the task of supporting the world's leading cyber power. To maintain airpower, the Air Force specifies new airframe capabilities and hires companies to build those very-specific planes for us. We hire contractors to erect base defenses to meet our specific physical-security requirements. Why is it then that the Air Force operates in cyberspace using software that wasn't developed for us and doesn't meet our security needs? The Microsoft products we utilize in the Air Force weren't created with security in mind. AFCYBER requires properly developed software created with security in mind that doesn't require billions of dollars to develop. That is where open-source software development comes into play. Open-source is defined by Symantec as organizations "that provide their product source code under the terms of a license that permits the licensee to use, alter, and redistribute the code" for free.[3] Adaptation of an existing version, or "distribution", of GNU/Linux could be bent to the security needs of the Air Force by community-driven contributions to the source code.[3]

DESCRIPTION OF ISSUE

1. The proprietary software we utilize is not suited for a secure enterprise network because of improper code development, a plethora of exploitable vulnerabilities and the requirement to patch them. Proprietary software is typically created to popularize features, functionality, and usability on the widest scale possible.[1] Microsoft programs and operating systems are prevalent vendor-specific examples of just such proprietary software. Normal methods of developing software fail to produce the "high-quality, reliable, and secure software" that the Air Force requires and Microsoft is no exception.[4] Standard software development business processes don't include sufficient facilities to weed out weaknesses that our adversaries could possibly exploit.[4] Microsoft's maximum backwards compatibility, rapid development of user-friendly features and out-of-the-box default configurations continue to make it highly exploitable.[1] Since 1998, Microsoft has released an average of approximately 70 security bulletins each year.[1] In turn, each of these security bulletins addresses multiple vulnerabilities in Microsoft products giving us at least 280 flaws each year. Microsoft is to be commended for creating patches and updates for these vulnerabilities but many of these insecurities could have been avoided with proper development. This onslaught of vulnerabilities in the Air Force Global Information Grid's (GIG) core software destroys any network security we could have hoped to maintain and shows no sign of slowing down.[1] Patching and "retrofitting" our networks is necessary for the short-term but a long-term plan must also be devised to address our cyber security needs.[5] Security added on after-the-fact complicates 24 AF's ability to "extend, maintain, and defend the Air Force portion of the global information grid".[6] Improperly developed and highly vulnerable proprietary software that requires mission-crippling patching may be a primary concern for purchased software but cost is also a consideration.

2. In addition, Microsoft product insecurities are the cause of lofty costs we've incurred. This price tag far exceeds any benefit we may receive. To begin with, the Air Force has spent billions of dollars to incorporate enterprise licenses for operating systems and office automation tools into our information network.[2] The Air Force then incurs massive costs associated with computer or network security incidents borne of Microsoft flaws. These costs include time, resources, and funding spent in the forensic analysis, reporting, logistical coordination, and education that is spawned from each of these security incidents. There is also the almost incalculable cost of lost confidentiality, integrity, and availability of our data incurred by malicious or inadvertent exploitation of flaws in Microsoft code. All these obvious costs, in addition to less-quantifiable ones, have a crippling effect on the Air Force's ability to operate in cyberspace. The Air Force has failed to achieve dominance in this domain due to, in part, the costly and insecure foundation from which we operate.

RECOMMENDATION

1. The United States Air Force should explore developing open-source software to use on the Air Force portion of the GIG in addition to developing that open-source software in a "community" forum. Open-source software has distinct advantages over proprietary software and Air-Force-led community-driven software development would leverage the strengths of both to harden the defenses of the Air Force portion of the GIG.

2. First, we must understand what open-source software really is. Symantec defines open-source as projects or companies that "provide their product source code under the terms of a license that permit the licensee to use, alter, and redistribute the code."[3] This code is public and available for inspection and revision.[3] Another characteristic of open-source code is that it is free.[7] Open-source code can be modified and redistributed without paying any fees, rights, or royalties.[7] There are subtle exceptions from project to project but this underlying characteristic remains the same. Differences are determined by the license the open-source software is released under. The realm of software licensing falls short of a legal quagmire but can become complicated. To put it simply, there are two major types of licenses: Free Open Source Software (FOSS) and Proprietary Closed Source Software (PCSS).[8] FOSS licensing falls into two major categories: Open Source and Free Software Open Source licenses are very similar and compatible with each other but Free Software licensing is the least-restrictive of the two types and is also considered a specific type of Open Source license.[8] The differences between Open Source and Free Software licenses that are minute enough they are frequently used interchangeably will not be discussed here.

3. Now that we have a better understanding of open-source software and licenses, we can already see benefits over the proprietary software we currently utilize on the Air Force's Enterprise Network. The Air Force has but to choose an existing project developed under a FOSS license, whether it is an operating system or office automation suite, and adapt it for use on our networks. We have the freedom to choose any gradient between versions: cutting-edge or stable. There are no licensing issues or fees

associated with open-source products. We would no longer have to trust the vendor to find flaws and patch them. In addition to all this, the software is free for use. Any money spent with proprietary vendors towards enterprise licenses could easily be applied to open-source development. To prove the point, there are many successful examples of FOSS already being used throughout cyberspace. Sendmail, an email transfer program, is used on 80% of all email servers.[23] The Berkeley Internet Name Domain (BIND) is the most widely used Domain Name System (DNS) software on the Intemet.[23] The Google search engine uses a cluster of 10,000 Linux machines, Yahoo runs directory services using FreeBSD, many large movie production companies render special effects on Linux machines and on-line companies such as Amazon and E*Trade use Linux on their back-end computer systems.[23] Generally speaking, open-source software provides a much-better value than the proprietary software we currently use. The next question is, how do we develop this existing product to meet our enterprise needs?

4. There are many different roads the Air Force could travel with regard to open-source development. Who should develop our open-source code and how? It would be easy enough to create or hire a team of experts to this end. Contractors, security experts, Computer System Programmers or private firms could easily be tasked to develop such an open-source product. In fact, the Department of Defense (DOD) has already created a Linux distribution, booted and executed solely from volatile memory, for public use.[10] The Lightweight Portable Security (LPS) distribution was created from Linux Mint which was in turn derived from the very popular Ubuntu distribution. LPS was developed by the Anti-Tamper-Software Protection Initiative (ATSPI) with program management performed by the Air Force Research Laboratory (AFRL) under the Free Software license GNU Public License (GPL).[9] The DOD already uses many open-source tools, applications and operating systems but the development of its own FOSS to "protect critical DOD intellectual property from piracy, tamper, and exploitation by nation-state-class threats" is a big step in the right direction." LPS was designed for individual public use. The next logical step is to develop FOSS to replace proprietary applications and operating systems we currently use. AFRL is an obvious choice to manage such a project and ATSPI already has experience in hardening Linux distributions, but any effort to create an enterprise-wide FOSS operating system is a herculean undertaking. This sort of project would best be a community driven project. Linux itself was born to and grew up in a collaborative environment. Just such an environment could greatly assist ATSPI and AFRL in the development of security-focused FOSS for public use. A great many benefits are provided when a collaborative- style of development is used. First, the "computing community" at large is able to view your code, provide improvements, make suggestions, identify flaws and even eliminate bugs for you.[3] Bugs identified in this manner can likely be fixed the day following their detection.[12] The evolution of code developed in this way evolves and adapts faster than proprietary software.[21] Second, a small team of proprietary software developers will fall behind on "bug-spotting" and software enhancements compared to the collective brainpower of a broad community.[13] Third, anyone may contribute, but the owner of the project decides which improvements are included and which are not.[19]

Fourth, Lehman's laws of software evolution suggest that as a code development project grows in size, it becomes more-and-more difficult to add new code to the project.[18] Unlike proprietary, closed-source code-development, the evolution of the open-source development model exhibits a "strong rate of growth" over time.[20] The success of FOSS development is proof that large and complex community-driven projects can flourish and grow.[22] AFRL could easily leverage the advantages of collaborative development to spearhead FOSS code to strengthen the Air Force portion of the GIG. This would better allow the Air Force to attain cyberspace dominance from a position of strength.

COUNTERARGUMENT

1. There are many opponents to the open-source development model with many reasons to oppose widespread open-source development. Mostly, these individuals are advocates of obscurity and secrecy. One of the leading arguments is that were the Air Force to develop an enterprise network entirely run by open-source software, we would be even more vulnerable to attack than we are now. Adversaries, whether they are nation-state actors, criminals, or terrorists, would have full access to the code being utilized on our networks. Knowing that, they could better find vulnerabilities, develop exploits and better attack us through cyberspace. Since we use closed-source proprietary code, our adversaries must blindly fumble for vulnerabilities. This supposition couldn't be farther from the truth. Microsoft has given source code for Windows XP, Windows 2000, Windows 7, Windows Server 2000, Windows Server 2008, Office 2010, and SQL Server to the Russian Federal Security Service.[15] Russia isn't the only country that has had access to Microsoft code. Microsoft has a program, known as the Government Security Program, that has given "public sector bodies" in more than 30 countries access to its code.[16] Cambridge University security expert Richard Clayton admits that while viewing Microsoft's code could enable the discovery of security holes such that could be exploited, access to the source is not a prerequisite and it's unclear whether access to the source code makes it any easier.[15] In addition, Microsoft is not immune to being exploited, or "hacked", themselves.[17] Microsoft code has been stolen by criminals and their source-code is in the open.[14] As it turns out, Microsoft's supposedly closed-source, proprietary code base isn't as closed as many believe.

2. Another argument against enterprise-wide implementation of open-source software is a lack of support and training. Moving our networks from one vendor to another would be a massive change for a population that can barely utilize the current proprietary software we have. Any mention of "lack of support" is a myth. Community-driven software projects are nothing but supportive. The open-source business model counts on selling support and services to its customers. It’s the best way for open-source companies, like Red Hat and Canonical Ltd., to profit from software that is distributed for free. Purchasing support licenses may require funding but is still significantly cheaper than purchasing not only support from proprietary vendors, but also enterprise licenses. On the other hand, transitioning our workforce from Windows to a Linux-based environment would pose some challenges. Our core providers,

administrators and cyber security personnel wouldn't suffer much, as Linux is already part of their training. Our users, on the other hand, would face some significant difficulties in such a transition. Many of these problems could be mitigated with well-thought out change management practices. Furthermore, AFRL already has experience in making the Linux desktop look and act more like a Windows-environment in LPS, making it easier to adapt by our Airmen.

3. No one can deny that there will be challenges to such a large transition but with proper planning, training, and change management the Air Force could make the move to a cheaper and more-secure software platform. "We've always done it that way" can never be an argument to stay the course.

CONCLUSION

In conclusion, the Air Force operates in cyberspace from a weak and vulnerable network foundation. Closed-source proprietary software is improperly developed, and fraught with flaws, which proves to make it entirely too costly to maintain. Patching these security holes also takes a costly toll on Air Force resources that could be better utilized elsewhere. Open-source software has been shown to have significant advantages over its proprietary counterparts. This fact is evidenced by widespread adoption in the business sector. In addition, community-driven software development has been shown to be superior when compared to individual or group development. As with anything, there is a downside to using FOSS, but these issues are easily mitigated. The advantages of assigning an agency, such as AFRL, to develop open-source Air Force enterprise-wide software in a collaborative community-driven environment far outweighs any benefits we receive from the closed-source proprietary software, crippling our networks, and hampering our mission.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. McClure, Scambray and Kurtz, "Hacking Exposed 6: Network Security Secrets & Solutions," p. 158.
2. United States Government Accountability Office, "The Global Information Grid and Challenges Facing Its Implementation," p. 1.
3. McLean, "Published Source Code Does Not Equal "Open Source"," p. 1.
4. President's Information Technology Advisory Committee, "Cyber Security: A Crisis of Prioritization", p. 21.
5. President's Information Technology Advisory Committee, "Cyber Security: A Crisis of Prioritization", p. 23.
6. 24 AF Factsheet, p. 1.
7. The Open Source Initiative, "The Open Source Definition", p. **1.**
8. Van Reijswoud and De Jager, "Free and Open Source Software for Development".
9. ATSPI Technology Office, "Lightweight Portable Security (LPS) Public Edition (LPS-Public) User's Guide Version 1.3.0", p. 40.

10. Lightweight Portable Security, p. 1.
11. Software Protection Initiative, p. 1.
12. Perens, "Open Sources: Voices from the Open Source Revolution", Chapter 1.
13. Raymond, "The Cathedral and the Bazaar", p. 35.
14. Borland, "Microsoft sues over source code theft", p. 1.
15. Espiner, "Microsoft opens source code to Russian secret service", p. 1.
16. Kable, "UK government joins Office source-code scheme", p. 1.
17. Bridis, "Microsoft hacked! Code stolen?", p. 1.
18. Godfrey and Tu, "Evolution in Open Source Software: A Case Study", p. 131.
19. Ibid, p. 132.
20. Ibid p. 134.
21. Weber, "The Success of Open Source", p. 2.
22. Ibid, p. 3.
23. Ibid, p. 6.

BIBLIOGRAPHY

24th Air Force Public Affairs, *24 AF Factsheet,* April2010. http://www.24af.af.mil/library/factsheets/factsheet.asp?id = I5663

ATSPI Technology Office, *Lightweight Portable Security (LPS) Public Edition (LPS-Public) User's Guide Version 1.3.0,* Distribution A, 5 January 2010. www.spi. dod.mil/docs/lpsmanual.pdf

Borland, John, *Microsoft sues over source code theft,* cnet.com, 27 September 2006. http://news.cnet.com/Microsoft-sues-over-source-code-theft/21 00-1025 3-6119892.html

Bridis, Ted, *Microsoft hacked! Code stolen?",* 27 October 2000. http://www.zdnet.com /news/microsoft-hacked-code-stolen/111513

De Jager, Arjan, Victor Van Reijswoud, *Free and Open Source Software for Development: exploring expectations, achievements and the future,* Volume 5, pp. 48-49. http://www.polemetrica.com.

Espiner, Tom, *Microsoft opens source code to Russian secret service,* zdnet.co.uk, 8 July 2010. http://www.zdnet.co.uk/news/security/2010/07/08/microsoft-opens-source-code-to-russian-secret-service-40089481I

Godfrey, Michael W., and Qiang Tu, *Evolution in Open Source Software: A Case Study,* 2000 IEEE International Conference on Software Maintenance, (Los Alamitos: The Institute of Electrical and Electronics Engineers, Inc., 2000).

Kable, *UK government joins Office source-code scheme,* zdnet.co.uk, 20 September 2004. http://www.zdnet.co.uk/news/desktop-os/2004/09/20/uk-government-joins-office-source-code-scheme-39167166/

Kurtz, George, Stuart McClure, and Joel Scambray, *Hacking Exposed 6: Network Security Secrets & Solutions,* l0th Anniversary Edition, (New York: McGraw-Hill, 2009).

McLean, Doug, *Published Source Code Does Not Equal "Open Source",* Symantec.com, 29 December 2010. http://www.symantec.com/connect/blogs/published-source-code-does-not-equal-open-source

Open Source Initiative, *The Open Source Definition.* http://opensource.org/docs/osd

Perens, Bruce, *Open Sources: Voices from the Open Source Revolution,* 1st Edition, (Richmond: O'Reilly, 1999). http://oreilly.com/catalog/opensources/book/perens.html

President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization,* February 2005. http://www.nitrd.gov /pitac/reports/20050301cvbersecurity/cybersecurity.pdf

Raymond, Eric S., *The Cathedral and the Bazaar,* version 1.31, (Sebastopol: O'Reilly Media, 2001).

United States Government Accountability Office, *Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation,* July 2004.

Unknown, *Lightweight Portable Security,* distrowatch.com, 16 November 2011. http://distrowatch.com /table.php?distribution=lps.

Unknown, *Software Protection Initiative.* http://spi.dod.mil

Weber, Steven, *The Success of Open Source,* (Cambridge: Harvard University Press, 2004).

The Importance of Certifying Systems in Support of ITW/AA
Major Pam Zane, U.S. Air Force (USSTRATCOM/J65)

ABSTRACT

This paper highlights the importance of certifying systems in support of the Integrated Tactical Warning and Attack Assessment (ITW/AA) system. General Kehler, Commander, United States Strategic Command, recently briefed the Senate Committee on Armed Services that "the nuclear command, control, and communications (NC3) component of the nuclear deterrent force is the most problematic."[1] Basically, the concern is ensuring communications are continuously available and reliable from the President to the nuclear force through the ITW/AA system.[2] Due to the critical nature of the missions that use the ITW/AA system, it is paramount that any and all system modifications of existing hardware or software within, or interfacing with, the ITW/AA system meet the standards set within written guidelines from the Chairman Joint Chiefs of Staff (CJCS). These requirements drive the criticality for an independent assessment through system certification. History has also shown us the need for this type of assessment and the need to empower the ITW/AA integrator to enforce compliance with relevant CJCS Instructions (CJCSI).[3] Finally, testing requirements on a test system versus the live system introduce challenges because many of the ITW/AA components are legacy systems and require a separate test facility.

DESCRIPTION OF ISSUE

The importance of certifying systems in support of the ITW/AA system is a challenging issue. Certification has a negative connotation to many and so the term is avoided like a virus. History has shown the community the need for an integrator, yet the position does not have the authority to enforce the community to follow appropriate CJCSIs. Testing also introduces a whole new set of issues due to many of the ITW/AA systems are legacy systems and there is no sustainment arm to maintain them and require new systems to replace them.

1. The certification process is in direct support of USSTRATCOM Unified Command Plan and is mandated by the Chairman of Joint Chief of Staff.[4] ITW/AA's warfighting system consists of sensors, processing nodes, ballistic missile/command and control nodes and communications links used for nuclear decision-making. The system certification process provides the Commander, United States Strategic Command (CDRUSSTRATCOM) with assurance that a new system or system change satisfies system integrity requirements and is capable of accomplishing its assigned mission.[5] System integrity ensures the system will perform correctly, reliably, and within the timeframe required by the operational missions and not communicate ambiguous data to the operators.[6] Because of the level of oversight and nature of the mission, the certification process is extremely stringent to maintain the integrity of the system.[7] The operations community has expressed concerns with these procedures and the process and tries to find ways to circumvent the system. Bottom line, system certification is the conscience of the system so why would the operations community not want to follow the process.

2. During the Cold War North American Aerospace Defense Command (NORAD) reported to the national security advisor false warnings of Soviet missile attacks, which led to alert actions for US strategic forces.[8] As the result of the false events, the Chief of Staff of the Air Force directed an in depth review of all aspects of Air Force support provided to the Tactical Warning and Attack Assessment (TW/AA) system.[9] The principal finding of the review was that the

TW/AA elements were not recognized or managed as a complete system, lack of end-to-end TW/AA system and system interface engineering and lack of centralized configuration control.[10] This led to the creation of the System Integration Office and has moved around to different organizations over the years. The integrator has lost the top cover required to enforce systems adhere to the existing Chairman Joint Chief of Staff Instruction requirements. Due to budget constraints over the years this office has also downsized to an individual vice several individuals accomplishing this important mission. The lack of knowledge of the overall system is also a limiting factor in qualified personnel filling the position.

RECOMMENDATION

1. I recommend all systems should be certified and go through the same rigor as systems that touch the ITW/AA system. This would apply to new systems and modifications as well as legacy systems. A certification officer should be assigned to each system and it is the certifying officers responsibility to be involved early for the most efficient and effective execution of the certification process. This would ensure any issues are identified early enough for the acquisition and testing community to adjust if required. Involving the certifying officer early also ensures that there are no delays in certification. The certification officer should be involved during critical design reviews and test readiness review boards. During these test readiness review boards the testing methodology is outlined. At this point the certifying officer ensures the testing meets the operational requirements. The certifying officer must continue to get involved early while at the same time adapt to the changes ahead. Technology will continue to change at faster rates and certifiers must continue to ensure system integrity while allowing the implementation of new technology in a timely manner. With more and more total system performance responsibility-type contracts, the certifier must adapt to working more closely with contractors. In addition to certifying all systems, to support the certification cause, I would recommend the certification office move under the J3 for operational oversight.

2. The following is some history to explain why the integrator office was established and why it is so important. The system certification program was started in 1981 as a result of several false mass raid indications mentioned above. A NORAD computer had produced United States false warning and alert actions based on a nuclear exercise tape being left in the TW/AA system.[11] Basically, the information was simulating an attack into the live warning system. A special management review of the Air Force support to the then tactical warning and attack assessment system concluded that the TW/AA elements were not recognized or managed as a complete system. This led to the creation of the System Integration Office (SIO), which looked at everything from architecture, configuration control, technical performance, certification and testing of the entire TW/AA. The SIO reported directly to the Chief of Staff of the Air Force. In 1986, space was added to the TW/AA mission now integration was added to TW/AA. Over the years, the integrator function has been delegated downward and has lost the necessary visibility at the national level. I recommend, in order for leadership to respect the process and decision, this function be moved to the national level for proper oversight and visibility. The position should still hold the integrator title so there is just a single point of contact, but report to an office at the national level. The integrator requires broad knowledge of the ITW/AA system and must have the authority to guide the process and make any necessary changes.

3. Testing is a critical piece of the certification process. In order to assure operational availability, all hardware and software modifications to existing equipment within or interfacing with the ITW/AA system should be tested in the TDF which is the legacy space test bed.[12] This facility maintains a robust, isolated test environment for legacy space command and control systems. The current configuration of the TDF is unable to test against new systems because the TDF does not have all the equipment required. The testing from the TDF is handicapped by the fact it does not match fidelity of operational systems. Updating the TDF to emulate the main mission processors in Cheyenne Mountain complex and ensuring the same configuration of servers, communications and tech control interfaces will assist the testers in validating the ITW/AA system's integrity. The testing will ensure the integrity of changes to legacy space hardware and software prior to implementation in the operational environment. The certifier must actively participate in combined test forces to ensure tests include the necessary events to evaluate the system integrity. This is absolutely paramount for these mission areas.

COUNTERARGUMENT

There are many misconceptions in the space warning, strategic warning and missile defense communities that drive operators, testers, and the acquisition community to find loop holes in the certification process so the mission system and/or modifications do not need to follow strict CJCSI requirements. A few of the misconceptions to achieve system certification are:

a. The new ITW/AA mission system or interface would mandate use of specific communication paths

b. Compliance with ITW/AA tightly controlled change control procedures drives delays in delivery

c. System certification increases the cost of the program

All of these are incorrect and just that, misconceptions. System certification ensures the system achieves the mission capabilities for which it is intended without adversely impacting or degrading system integrity. The certification process does not drive the use of specific communication paths. The mission and system drives what paths will be required. Secondly, the change control procedures ensure the ITW/AA system operationally complies with the requirements identified in current CJCSIs. The purpose behind the strict change control is to ensure the changes are initiated, evaluated and implemented in a deliberative and structured process. This assures the overall system integrity and avoids the introduction of modifications that could degrade the operational capabilities of the ITW/AA system. The final misconception is that system certification increases the cost of the program. The certification process is not a fee for service; the process is conducted in parallel with development, testing and trial period activities. The necessity for certification is in what it prevents.

CONCLUSION

Certification is not an easy nut to crack. There are many issues and only a few of them highlighted above. The certification process runs in parallel with other processes and provides the CDRUSSTRATCOM with assurance that a new system or system change satisfies system integrity requirements and is capable of accomplishing its assigned mission. This provides the operational community the assurance that no ambiguous data is passed in the ITW/AA system to the operators. It also ensures the data is accurate, correctly processed, correlated, and received by the sensors and correlation centers. Finally, a robust integrated testing facility is desperately

needed to meet the needs of the ITW/AA mission. My recommendation to fix these issues is to communicate to leadership, testers, and the acquisition community that the system certification provides CDRUSSTRATCOM with the data confidence required to authorize the system for unrestricted operational use. General Kehler communicated USSTRATCOM's success will hinge on the effectiveness of the US response.[13] Maintaining the integrity of the ITW/AA system is crucial to meeting this challenge.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Kehler, Robert C., General, Statement before Senate Committee of Armed Services.
2. Ibid.
3. CJCSI 6811.01B, 2 Jul 07, current 27 Jul 08.
4. CJCSI 6210.02B, 1 Oct 07, current 10 Feb 09.
5. Ibid.
6. SI 534-22, 25 Mar 11.
7. SI 535-1, 25 Mar 11.
8. The 3 a.m. Phone Call, The National Security Archive, George Washington University.
9. Ibid.
10. Ibid.
11. The 3.a.m. Phone Call, The National Security Archive, George Washington University.
12. Ni 10-3, 1 Apr 09.
13. Kehler, Robert C., General, Statement before Senate Committee of Armed Services.

BIBLIOGRAPHY

CJCSI 6210.02B, *Information and Operational Architecture of the Integrated Tactical Warning and Attack Assessment System,* 1 Oct 2007, current 10 Feb 09.

CJCSI 6811.01B, *Nuclear Command and Control System Performance Criteria,* 2 Jul 07, current 27 Jul 08.

Kehler, C. Robert, General, *CDRUSSTRATCOM Statement to Senate Committee on Armed Services,* 27 Mar 12.

NI 10-3, *Mission Integrity, Change Control Management, and Test Control for the Integrated Tactical Warning and Assessment System,* 1 Apr 2009.

SI 534-22, *Mission Integrity, Change Control Management, and Test Control for the Integrated Tactical Warning and Attack Assessment (ITW/AA) System,* 25 Mar 11. SI 535-1, *USSTRATCOM System Certification Process,* 25 Mar 11.

The National Security Archive, George Washington University, *The 3 a.m. Phone Call.*www.gwu.edu/~nsaarchiv/nukevault/ebb371/index.htm.

Zane, Pamella J., Major, USSTRATCOM/J65 Systems Certification Officer.

The Importance of Software Assurance vs. Cost
SMSgt Issac M. Brown, U.S. Air Force (31 CS)

ABSTRACT

Every single day networks around the globe are probed, exploited or attacked through vulnerabilities related to software defects. These vulnerabilities present opportunities for skilled intruders to access information systems and networks, many times unnoticed to network users, thus providing gateways to critical data housed on such systems. One question asked by many software engineers and users alike is "How much are you willing to spend for a secured software application?" This will be the topic of this background paper. As an Information Technology project manager, I know the importance of the project team capturing as many, if not all, the requirements of a software project while staying within the guidelines of a project. Many times this results in the common and often encouraged practice of reusing code to save time and money, thus reducing initial cost for creating a software application. On the other hand, you could have a team write all the code from scratch, test, and verify software assurance which would significantly increase cost.

DESCRIPTION OF ISSUE

1. The security of Information Systems is at risk when software is produced and released to maintain budgetary constraints versus producing high quality products. An example of this would be the recent government warnings concerning an insecurity found in Oracle's Java software.[1] As noted in an article published on USAToday.com the following warning was given with regards to the highlighted security risk:

> The flaw in Java 7 "can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system," (Winter, 2013)

The article further outlines how hundreds of millions of computer users could be the target of potential hacker attacks seeking to exploit systems with malware or other malicious code. This opens consumers to identity theft or to become part of botnets used to conduct denial of service attacks on other information systems. The software giant Oracle is not known for taking shortcuts due to budgetary concerns, but this is just one of many software vulnerabilities placing an untold number of information systems, 300 billion by Oracle's estimates, at risk for exploitation. The same version of Java 7, update 10 also contained another vulnerability noted by U.S. CERT but was not published as part of the public warning.[2] Oracle quickly released an update addressing both vulnerabilities, but U.S. CERT still advised users to disable Java even after applying update 11 to mitigate the potential for exploitation of other vulnerabilities. Java is one of many software applications used to present data to consumers all over the Internet and such vulnerabilities could have resulted in a loss of information.

2. The amount of data lost due to compromises of information systems can cost an organization more than producing software with less vulnerability thus reducing the opportunity for theft. As noted in the Java example, software vulnerabilities increase the opportunities for theft. The computer security company McAfee published a white paper detailing the effects of data loss on companies and consumers alike. A highly publicized data breach occurred in 2011 involving Sony Corporation.[3] In early 2011, Sony's Playstation Network was compromised resulting in the loss of over 77 million records.[4] The famed network which allowed a number of services including on-line gaming, music, movie and game downloads and other Internet content

was off-line for over two weeks while Sony tried to recover from the incident. According to CNET, the attack was very sophisticated as indicated in the following excerpt:

> …Unnamed person illegally gained access to Sony's PSN servers in San Diego, Calif., by hacking into an application server behind a Web server and two firewalls. According to Sony Chief Information Officer Shinji Hajesima, the attack was disguised as a purchase, so it did not immediately raise any red flags. The vulnerability the attacker was able to exploit was known, according to Sony.

Sony Corporation was recently fined 250,000 pounds, almost $385,000 by the United Kingdom Information Commissioner's Office for its failure to protect the information of UK citizens.[5] This fine does not account for the thousands of dollars in revenue Sony lost during the network outage lasting over two weeks or the money and incentives paid to customers whose data was compromised. Sony has yet to detail what vulnerability was used to pull off such an elaborate loss of electronic information.

3. Applications that are not designed with requirements for the protection of data being stored or manipulated are vulnerable to similar breaches. The U.S Air Force provides an example of not clearly defining requirements for software design with the recent failure of an enterprise resources planning project.[6] The Air Force project had incurred over $1 billon in cost since inception in 2005 and was recently scrapped after realization it would not yield the benefits based on the money invested. Enormous costs associated with information technology projects are normally the result of failure to define clear project requirements or a subset of project creep, the ever-expanding project goal. Analyst Michael Krigsman, CEO of consulting firm Asuret and an expert on why IT projects fail, stated the following with regards to such endeavors:

> …Preventing more major project failures will be extremely difficult to accomplish, Krigsman said. Fundamental problems exist in the entire chain, from defining the project, through procurement, delivery, staffing, and oversight." (Kanaracus, 2013)

Krigsman's bleak outlook on information technology projects is attributed to the fact that most teams go into the project with a set of undefined or lack of clearly stated goals. Teams are usually defining goals and requirements as the project moves forward thus ballooning cost until either the project fails or produces a product loosely meeting expectations of the consumer.

RECOMMENDATION

4. Software vendors should develop applications capable of meeting stringent quality control measures while striking a balance between reliability and security. Companies need to be innovative with software development enhancing security measures and reducing the reliance on patch management to correct software deficiencies. Patch management has become the normal in software development. The following excerpt was taken from the U.S. Department of Homeland Security:

> Sound practices are more effective and appropriate when they address (help prevent, mitigate, etc.) classes of problems. Detailed fixes to specific problems are not sound practices. For example, we do not provide security patches on this site. However, we do discuss detailed coding techniques that could be used during development to help prevent problems (Department of Homeland Security, 2013)

This section is part of seven objectives detailed by the Department of Homeland Security (DHS) in its effort to improve Software Assurance. DHS has been charged by the U.S. Government to help protect critical infrastructure and has taken a public awareness approach to doing so. The DHS Office of Cybersecurity and Communications published these seven steps to software assurance in order to assist those in software development to produce quality projects with little vulnerabilities.[7] It all comes down to risk analysis. Companies cannot fail to conduct effective risk analysis on software projects. Failure in these areas result in releasing software to the public with known vulnerabilities in hopes they are not discovered or corrected in a timely fashion after being discovered. Neither option is conducive to consumer security as these vulnerabilities could and have resulted in the loss of critical information throughout the world.

5. Companies should safeguard data stored on information systems using various technologies including data encryption and must move quickly to correct software vulnerabilities once identified. BitLocker, a drive encryption tool, was created by Microsoft to provide the common computer user the ability to secure and safeguard data stored on personal computers.[8] The technology was created in response to data stolen through physical means or through software vulnerabilities. While not foolproof, BitLocker offers a level of assurance to the average consumer that their data is relatively safe if used properly. The fictional character Bruce Wayne used a formidable encryption algorithm to secure contingency plans for members of the Justice League should the need ever arise to neutralize them. In this cartoon world, the character also realized just one level of security was not enough and built a failsafe if his encryption was ever compromised; calling back to the Bat Cave once the encryption was broken. While this is fictional, it could give companies a basis to develop higher security measures built into their software such as notifying the consumer or corporation when data has been accessed on servers not associated with the software. Technology offers many possible solutions to secure data stored within and accessed by software applications. Companies have become accustomed to using one level of security to protect data such as just using 128-bit encryption, or some other method of security but not fully investing into combining measures to make it difficult for thieves to access data if the software application is compromised. Dr. Sheldon stated in a briefing to Cyber 300 class in October of 2012 "the adversary always has a vote."[9] His quote was referring to those wishing to gain access to critical information systems will always play a part in how you defend such systems. Vendors must account for the actions of the adversary when detailing and incorporating security measures for protecting user information.

6. A clear definition of application requirements is needed before projects are commissioned. Security measures cannot be an after-thought in software development and design, but must be incorporated into application requirements to ensure software assurance is addressed. It is imperative for the success of any project that requirements are clearly defined before the project begins. "IT projects are difficult to estimate…" according to Keri Pearlson & Carol Saunders (2010) authors of Managing and Using Information Systems. These types of projects usually involve a vision of what the project owner wants in the end product and many project teams fail to scope and define the vision into a tangible and obtainable requirement or goal. The two authors go on to say project failures are attributed to poor estimating techniques and many teams feel they can just throw more manpower at the project to incorporate missing or undefined requirements later on in software development.[10] Security measures are often the most overlooked aspect of software applications. The focus is on what the software is designed to do, such as automated data processing, providing financial calculations or coordinating airstrikes on

multiple targets. Companies don't take the required amount of time thinking about the vote an adversary has on whether their software performs its mission as required. Information Technology projects must include security measures as an inherent function of the software platform as much as the overall mission of the software itself. For example, if Adobe Incorporated failed to include security measures in its Adobe Acrobat Reader, the .pdf file format would be a vector for hackers to infect systems worldwide because of the file format popularity in digital media. Adobe has realized security is a function of its software just like the ability to create, read, and modify the .pdf format. Security measures need to be one of the top three functions listed whenever software requirements are considered during the planning phase of any IT software application project.

COUNTERARGUMENT

7. Software vendors lose market share and money when software releases are delayed due to programming requirements. This is a fact of business. The Windows operating system would not have almost 90% of the market share in terms of personal computers in the world if Microsoft did not release a new version of the famed operating system (OS) every couple of years.[11] Relevancy plays an important part in a company's decision to release software applications containing vulnerabilities. It was almost seven years between the release of Windows XP and Windows Vista. During this time period Microsoft watched as competitor Apple gained some ground in the market by releasing updates to their operating system. Microsoft delayed releasing Vista because of compatibility and vulnerability issues which plagued the software even after its release. While the damage was not sufficient to ruin Microsoft Corporation, it did tarnish its reputation. The software vendor had to quickly release another version of the Windows operating system to try and regain lost ground. They did so by releasing Windows 7, an OS many claimed to be the best one provided by the long-standing software company. Windows 7 solidified Microsoft's foothold on the personal computer (PC) marketplace with an amazing 44% of current PC owners using the operating system. If Microsoft had delayed the release of Windows 7 after the failed iteration of Vista, it could have seen more people move to either the free OS called Ubuntu, a version of Linux, or towards the more expensive Apple products. These are decisions software companies must deal with to ensure they remain relevant in a quickly changing environment known as software applications.

8. Technology changes make it nearly impossible to anticipate all security flaws in software development. As mentioned earlier in this paper, Oracle released an update of Java which included two zero-day vulnerabilities.[12] Whether the software company knew of these vulnerabilities is unknown, but the argument can be made that technology changes at a pace the software producers have a difficult time keeping abreast with. Updates are usually produced to enhance features, including security measures lacking in the previous version. Thinking again of the vote an adversary has on whether or not a software application is successful at its mission, a company cannot successfully anticipate all the changes in the world of technology. Many hackers could successfully circumvent any security measures put in place by software vendors simply because they have the time to dedicate in cracking their code and exploiting both known and unknown vulnerabilities.

9. Companies using effective risk management in developing software applications will minimize cost incurred to users for software development. Again looking at the example of Microsoft, the company has developed an effective system of patch management. Microsoft uses

patch management as part of its risk management when deploying new software applications. Effective risk management could potentially minimize the loss of data when software is used by the consumer. Sony used risk management effectively when they noticed the first breach in security for the PlayStation network. The company decided to keep the network offline as they focused on fixing the first vulnerability discovered. In Sony's case, they were unaware the first attack was just a probe for the second more brazen attack resulting in the compromise of so many records. Risk management should take into account all the known risks involved with releasing software applications. Effective testing and evaluation will show weaknesses in software applications and the project team as well as the company could decide on whether the software is ready to be released.

CONCLUSION

Software assurance plays a key role in protecting data stored on networks and IT systems around the globe. Vulnerabilities in these applications are commonly targeted and exploited by attackers to gain access to data once thought to be held securely by the software application. The cost of securing these vulnerabilities should be included during software development. The price of releasing applications with vulnerabilities could be far greater than trying to secure the application before its release. Security testing should also be a part of each software application or platform project. Major companies such as Oracle, Microsoft, and Sony have seen both positive and negative effects of releasing software before it was ready for the public. Others could contend these companies had no way of knowing their software contained vulnerabilities able to be exploited in the manner they were. In the world of software development, risk management and the bottom line play an important part in the decisions Chief Executive Officers make to press forward with projects for software applications. Many software developers are focused on releasing applications to remain relevant in an ever-changing IT world and passing the risk of data compromise to the application users. These developers also rely on patch management to close or contain vulnerabilities once discovered, which in many cases occurs when data has been lost or stolen. Software quality and security are key components to successfully protect data used on an information system and should not be sacrificed solely on the principle of saving money alone.

REFERENCES

1. Winters, Michael. http://www.usatoday.com/story/tech/2013/01/11/homeland-security-disable-java-security-vulnerability/1828011/
2. Security, Department of Homeland. "Java 7 fails to restrict access to privileged code."Vulnerability Notes Database - US CERT. http://www.kb.cert.org/vuls/id/625617
3. Ogg, Erica. "The PlayStation Network breach." CNet. http://news.cnet.com/8301-31021_3-20058950-260.html 4 (accessed April 11, 2013).
4. Ibid.
5. Zorz, Zeljka. "Sony fined £250,000 for 2011 Playstation Network breach." Help Net Security. http://www.net-security.org/secworld.php?id=14295
6. Kanaracus, Chris. "Senate to probe failed Air Force software project as lawmakers call for stop to IT waste." IT World. http://www.itworld.com/software/338401/senate-probe- failed-air-force-software-project-lawmakers-call-stop-it-waste?page=0,0
7. Jarzombek, Joe. "Seven Objectives of Software Assurance Sound Practices." Build Security In. https://buildsecurityin.us-cert.gov/bsi/dhs/92-BSI.html

8. Microsoft Corp. “BitLocker Drice Encryption Overview” Windows Server. http://technet.microsft.com/en-us/library/cc732774.aspx
9. Dr. John Sheldon. “Cyberpower and Strategy.” Center for Cyberspace Research, Air Force Institute of Technology.
10. Pearlson, Keri, and Carol Saunders. Managing and Using Information Systems. Hoboken NJ: Wiley, 2010
11. Whitney, Lance. “Windows 8 swells to 2.7% of OS market” CNet. http://news.cnet.com/8301-10805_3-57572003-75/windows-8-swells-to-2.7-of-os-market/
12. Ogg, Erica. "The PlayStation Network breach." CNet. http://news.cnet.com/8301-31021_3-20058950-260.html

PART IV: POLICY AND DOCTRINE

Cyber Superiority: Myth or Reality
MSgt Michael R. Woolingham, U.S. Air Force (NRO)

ABSTRACT

Since 1947 the Air Force has prided itself on dominating every aspect of war it embarks on. From air to space, whether in a support role or the main player, the same goal applies: superiority through dominance. It is crucial not only to the success of the mission but to the survivability of our nation.

In 2005, the cyberspace domain was added to the Air Force mission statement and amended in 2007 to include the words "*fight and win.*" These words imply the continued performance expectation of superiority not only in air and space but now in cyberspace. Unfortunately, the level of superiority senior Air Force leadership has come to expect in air and space cannot be achieved in cyberspace.

The Air Force has achieved mastery of the first two domains because the physical properties and laws applicable to both are well known. They are domains that have boundaries and can be observed and measured. However, in cyberspace, due to the complexity, interconnectivity, ever-changing landscape, and numerous threats, this is not possible. It is this idea that constitutes the thesis of this paper: cyberspace superiority, as defined in Air Force Doctrine Document (AFDD) 3-12, is not achievable.

DESCRIPTION OF ISSUE

1. There is no denying the critical importance of technology in our modern society and military operations. From online banking to attacks on Supervisory Control and Data Acquisition (SCADA) networks, cyberspace is the medium by which it can occur. It is a highly contentious domain that provides access to desirable assets of the United States by would be foes. Consequently, protecting those assets in this domain is one of the nation's top priorities. The Center for Strategic and International Studies Commission on Cyber Security for the 44th Presidency indicated as its central finding that the United States must treat cyber security as one of the most important national security challenges it faces.[1]

2. In order to properly defend or function in the cyberspace domain, one must first fully understand its weaknesses, its ability to proliferate, and one's effective span of control over it. Network intrusions, data exfiltration, malicious logic, host enumeration, and malware are 21st century words to describe an age-old dilemma. The enemy wants information and information assets in order to gain an advantage, and they will attempt to get that information by any and all means available to them. Connected information systems and the data traversing them make this possible by providing an opportunity for exploitation. Many historical examples exist to support this. In 1876, Alexander Graham Bell is credited with inventing the telephone.[2] Shortly thereafter in 1890, wiretapping was invented to exfiltrate conversations from this new technology.[3] In 1969, the first electronic message passing network, the Advanced Research Projects Agency Network (ARPANET) was created by the Department of Defense (DOD).[4] Only two years later in 1971, the first virus, the Creeper Worm written by Bob Thomas, exploited ARPANET.[5] Historically, with each new technology comes a manner in which to exploit it.

3. The Air Force mission is to fly, fight and win...in air, space and cyberspace. It has time tested doctrine and vision statements to support air and space domain operations with a proven track record of success, but not in cyberspace. The problem centers on how aspects of the domain are defined. It is the definition of a domain that helps formulate policy which ultimately affects implementation and the mission. The Air Force is attempting to utilize its success in air and space as a template for cyberspace; specifically, as it pertains to superiority. This is not only futile but unrealistic.

4. AFDD 3-12 Cyberspace Operations defines cyberspace superiority as "*the operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference*".[6] What AFDD 3-12 fails to do is scope it, indicate how to measure it, and conclusively determine if it has been accomplished. Mission planning incorporates the aspect of superiority as a decision point and as such for cyber operations, it's unachievable as defined.

5. The Air Force establishes dominance and superiority in air and space based on our ability to control those domains. If the mission is accomplished with minimal adversary interruption while operating through those domains, then it is deemed that the Air Force has superiority in those realms. In air and space, dominance is relatively easy to measure due largely to the fact that there are specific boundaries, it can be visualized, and total destruction within those domains is not needed to ensure superiority.

6. Boundaries provide clarity of where the requirement of superiority must be accomplished. It indicates a given range by which freedom to attack and freedom from attack is enjoyed. It also establishes the area in which the adversary is restricted from the same.

7. Boundaries within air and space are known. It is well established where one nations land borders and air space begin and another ends. AFDD 1 Air Force Basic Doctrine scopes air superiority by stating that "*Air superiority provides freedom to attack as well as freedom from attack.*"[7] The Air Force achieves air superiority through an impenetrable defense within a given range or Area of Responsibility (AOR). This is routinely seen within military operations such as Operation Northern Watch and Operations Southern Watch in which the Iraqi Air Force was restricted to flying operations within specific coordinates. The AOR provides the specific area in which air superiority is required. The level of superiority obtained further dictates mission actions taken by the Combatant Commander (CCDR). If the level of superiority is not achieved within the AOR to facilitate further operations, then actions are taken to raise the level. If actions are taken and the level of superiority is not as reported, disaster is certain to follow.

8. With regards to boundaries in space, this becomes a little more difficult but not impossible. AFDD 2-2, Space Operations defines space superiority as the "*degree of control necessary to employ, maneuver, and engage space forces while denying the same capability to an adversary.*"[8] As with air, there is a definite starting point at which the atmosphere transitions to what is commonly referred to as space. This beginning facilitates a boundary. With a boundary an AOR can be created, hence an area of required superiority can be established.

9. Visualization, the second aspect, is a measurement of confidence. It is not just what can be seen with the eye but also seeing the bigger picture through other methods. It is the act of having

empirical data which influence our decisions. For example, as humans, we look to the weather report to decide if an umbrella may be necessary. If the weather report indicates a chance of rain, then prudent action would be to carry an umbrella. That said, upon exiting a building, the umbrella is not indiscriminately deployed. Instead, if rain drops are felt or seen then the umbrella is used. It is only when there is empirical data of the rain falling that the umbrella is used.

10. Visualization is often performed on air and space domains by the theater commander through battle damage assessment intelligence reports and satellite pictures indicating the level of superiority obtained in these domains of war. This intelligence provides the empirical data necessary to be able to make operational, strategic, and tactical decisions for executing the mission. Without the tools to provide the visualization and insight into the level of superiority achieved in the air and space domains, those decisions would not be possible. By having that visibility, the CCDR can then make the determination of the level of superiority achieved thereby being able to determine the next course of action to take.

RECOMMENDATION

1. Physical boundaries and visualization strategies are straight forward to measure as it pertains to the air and space domains. However, in cyberspace, this is not the case. Boundaries in cyberspace are not easily delineated and visualization techniques are only accurate for that moment in time. Ultimately, this makes establishing cyberspace superiority difficult at best.

2. Due to the connected nature of cyberspace, defining boundaries is impossible. Cyberspace does not meet the conventional aspects of the physical domains of air and space. Therefore, establishing boundaries that are universally recognized is not possible. There are IP ranges that are registered and used in a specific country. This provides some semblance of a boundary but what about if an attack comes from a location outside the registered IP range for that country? Additionally, technologies exist to obfuscate and spoof source addresses such that an attack could appear to be coming from some part of the world when in fact it originated from somewhere else. How can superiority be accomplished when attribution is nearly impossible? With all this uncertainty how can one begin to direct superiority of cyberspace when an AOR cannot even be determined conclusively? There may be the desire to retaliate but if the source of the cyber-attack is unknown or spoofed, that may not be an option. To take action without certainty could result in disaster.

3. Visualization strategies can also prove to be just as difficult to create. Cyberspace is constantly in a state of change. The manmade domain was created to be “self-healing” without a single point of failure. Additionally, nodes are added and removed with minimal effort or affect to the cyberspace domain. This calls into question the accuracy of mapping or visualizing the IP range of interest. That’s not to say that at the moment the visualization method was implemented that it wasn’t correct but that it could change immediately upon completion without much notification.

4. Cyberspace is in a constant state of change. Any doubt with regards to superiority when it pertains to the site picture of an adversary is not conducive to successful mission operations. The level of superiority achievable directly affects the courses of action presented to the CCDR. If that is skewed or improperly presented, the results could be catastrophic.

COUNTERARGUMENT

1. If the current Air Force definition of cyberspace superiority is unachievable, as indicated by the author, then a possible counter to this could be domain elimination. British Air Chief Marshal Sir Arthur Tedder stated that air superiority "*is a campaign rather than a battle and there is no absolute finality as long as enemy aircraft are operating*."[9] To truly be superior in cyberspace, as defined in air and space, the United States must be the only users of the realm. All others must be completely stopped. This can cause significant consequences whether planned or otherwise.

2. It is unrealistic to expect that cyberspace can be controlled to the point where no adversary cyber-attack is possible. Most end devices have the potential to serve as a platform for launching a cyber-attack. Even if the physical infrastructure of enemy cyberspace is completely destroyed, it is still possible for a cyber-attack to originate from outside the area of conflict. In cyberspace the infrastructure and end devices are the domain. Eliminating the infrastructure eliminates the domain and also the ability to continue intelligence collection on the adversary. The author believes that eliminating the domain doesn't necessarily win the war. As Sun Tzu said in the Art of War, "*In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to recapture an army entire than to destroy it.*"[10]

3. Unlike air and space superiority, eliminating enemy cyber forces does not achieve a proportional benefit in cyberspace. Cyber-attacks can originate from many sources and it is impossible to locate and eliminate all of them. Enemy cyber forces can also easily disguise their point of origin. Additionally, other non-military parties who are sympathetic to our adversaries could still launch attacks. These vestiges of resistance would continue to operate and pursuing them could prove just as difficult as pursing traditional gun carrying insurgents.

CONCLUSION

1. In order to properly defend our cyber infrastructure, personnel must be hyper-vigilant in order to nullify cyber-attacks, more so than in the other warfighting domains. This is due to the enormous size, complexity and connected nature of cyberspace. Since adversaries can very easily go unrecognized, a sophisticated, active defense is critical to allow the United States to fight through cyber-attacks. Enemy attacks will occur, and our defenses must be strong enough to withstand them so we can fight through the attacks.

2. Cyber-attacks over the past couple of years have increased in their scope, depth, and sophistication and many nations have become victims. In defense of those nations, it is hard to establish attribution in a domain that has so many connections. The packets that flood the network every day do not carry a header file indicating from which country it was initiated from. Although this would be nice, the lack of a distinguishing bit is the reason our adversaries can attack and hide in the same place at the same time. Without an established AOR or the ability to have a reliable sight picture of the domain, it is impractical to attempt cyberspace superiority as defined in AFDD 3-12.

3. Whenever atrocities occur, it typically only affects and motivates a response from those close to ground zero. Whether the event is on the other side of town or the other side of the world, it's

easy to empathize with the victims and it's just plain foolish to think it can't happen to the U.S. On September 11, 2001, our world changed. Prior to that date, we believed that the U.S. was safe from an attack on U.S. soil. We thought that the sheer size of the U.S., the success of our nation and military, our geographic isolation, and the influence we had on the world could insulate us from direct attack. These factors no longer protect the U.S. from attacks. In order to meet our nations call to action, the Air Force must first secure its foundations in cyberspace. Because cyberspace superiority is not achievable as currently defined, the Air Force must build the strongest cyberspace defense possible and develop the ability to fight through enemy attacks to accomplish the mission. In doing so, this will allow the Air Force to pick the time, place, and manner necessary to continue protecting national interests to fulfill the mission. Only when we adopt this methodology will we truly be able to have cyber superiority. Cyberspace has truly fulfilled the cliché of "it's a small world". For with the stroke of a key, nations can be brought to their knees.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Securing Cyberspace for the 44th Presidency, 2008
2. Casson, "The History of the Telephone", p. 15
3. Ibid, p. 27
4. Computer History Museum, http://www.computerhistory.org/Internet_history
5. Ibid
6. AFDD 3-12, p. 2
7. AFDD 1, p. 76
8. AFDD 2-2, p. 7
9. AFDD 1, p. 42
10. Sun Tzu, "The Art of War", p.54

BIBLIOGRAPHY

James A. Lewis, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, 8 December 2008, http://www.csis.org/publication/securing-cyberspace-44th-presidency (accessed 11 May 2012).

Herbert N. Casson. "The History of the Telephone", 27 August 1910.

"Computer History Museum", http://www.computerhistory.org/Internet_history (accessed 12 May 2012).

Air Force Doctrine Document 3-12, "Cyberspace Operations", page 2, 15 July 2010.

Air Force Doctrine Document 1, "Air Force Basic Doctrine", page 76, 17 November 2003.

Air Force Doctrine Document 2-2, "Space Operations", page 7, 27 November 2006.

Air Force Doctrine Document 1, "Air Force Basic Doctrine", page 42, 17 November 2003.

Sun Tzu, "The Art of War", Harrisburg, USA: Military Service Publishing Company, 1944.

Making One Person the Commander of U.S. Cyber Command and Director of National Security Agency Creates a Conflict of Interest

Lt Col David L. Stevens, U.S. Air Force (Headquarters, Air Force Space Command)

ABSTRACT

The decision to dual-hat General (GEN) Keith B. Alexander as Commander, U.S. Cyber Command (USCYBERCOM) and Director, National Security Agency (DIRNSA) created a fundamental conflict of interest due to the responsibilities inherent in both positions.1 The USCYBERCOM Commander must lead military operations as directed by the President and Secretary of Defense under Title 10 of the U.S. Code. However, DIRNSA must lead intelligence operations supporting both national decision makers and unified commands under Title 50.[2] Additionally, DIRNSA must provide support to all unified and sub-unified commanders as a combat support agency (CSA).[3] Currently, GEN Alexander is required to support himself creating an inherent conflict of interest and potentially degrading the support the National Security Agency (NSA) provides to the other combatant command (COCOM) commanders as well as all the agencies and departments of the U.S. Government (USG).[4] Finally and based on the description found in the President's Fiscal Year 2013 (FY13) Budget, the National Intelligence Program (NIP) probably funds a significant portion of NSA's cyber workforce.[5] In a severely constrained fiscal environment, GEN Alexander has to decide whether or not his forces should conduct NSA missions or USCYBERCOM missions which probably has an inhibiting effect on the development, growth, and maturation of the service components assigned to USCYBERCOM.. Therefore, the best course of action is to clearly separate the positions of Commander, USCYBERCOM and DIRNSA.

DESCRIPTION OF ISSUE

1. When the decision was made to activate USCYBERCOM as a sub-unified command under U.S. Strategic Command (USSTRATCOM), a parallel choice was implemented to put the responsibilities of both Commander of USCYBERCOM and DIRNSA under the same general officer. Making one person both Commander of USCYBERCOM and DIRNSA creates a conflict of interest between the military and intelligence responsibilities inherent in those jobs. No matter who is appointed to fill those roles, there will always be a pull between the continuous demands of the intelligence mission and functions that require answers to national security questions versus the operational mission of USCYBERCOM to develop, plan and execute military missions at the direction of the President of the United States (POTUS) and the Secretary of Defense (SecDef) in support of national security strategy and objectives.[6]

2. Title 10 of the U.S. Code governs military operations conducted by USCYBERCOM while Title 50 is the legal foundation for intelligence operations conducted by the NSA.[7] During Phase 0 shaping operations (also known as foundational or steady state operations), Title 10 functions primarily focus on planning (both deliberate and crisis action) to prepare for future military operations and shaping activities such as theater security cooperation in building both trusted relationships and partnership capacity.[8] Except in extended counterinsurgency (COIN) and anti-drug operations, most military actions ordered by the POTUS in his role as Commander in Chief (CinC) are of relatively short duration due to the desire for quick military victory and a return to Phase 0 where the military instrument of power is not the primary tool of statecraft. In contrast to the Title 10 responsibilities of USCYBERCOM, the National Security Agency/Central Security Service (NSA/CSS) has a prominent and never-ending role throughout all Phases of

conflict especially during Phase 0 for shaping of the battlespace. Intelligence operations are required continuously in order to prevent strategic or operational surprise, to inform the POTUS, SecDef, and other key decision makers (such as the National Security Council) as to the disposition, capabilities, and intentions of other nation states, non-state actors, and transnational forces and trends that may threaten U.S. national interests (not just national security objectives).[9] If anything, intelligence operations at NSA/CSS during Phase 0 are more critical than other Phases since they can help prevent conflict from occurring and preserve our military capabilities for essential operations when our national interests are at stake and require the commitment of U.S. armed forces.

3. Since the NSA/CSS is a CSA, DIRNSA must provide support to all unified and sub-unified commands primarily through the CSS.[10] In the current construct, GEN Alexander is a customer, as the USCYBERCOM Commander, to himself, as the DIRNSA. One could easily argue that this gives the Commander USCYBERCOM a special relationship with NSA/CSS that potentially degrades NSA's support to all the other COCOMs. At the very least, the same person is charged to lead Title 10 operations that focus on military planning and operations versus Title 50 intelligence operations which are focused on gaining access, collecting information, conducting analysis, and answering questions for national decision makers and COCOM commanders alike.[11] These two missions could easily come into conflict when evaluating desired effects because a Title 50 entity would focus on value of intelligence gained versus the loss of a source or access to intelligence information whereas a Title 10 organization would place more value on creating desired effects in the battlespace to achieve military objectives supporting achievement of the end state outlined in a named military operation.

4. Current fiscal constraints primarily caused by the economic downturn and potentially exacerbated if Congress does not prevent sequestration this year which would cut an additional $500 billion from the Department of Defense (DOD) budget[12] put human resources at a premium for both CSAs and the military services. Whereas the military personnel billets are primarily funded through their respective portions of the DOD budget, a large portion of DOD's cyber-human resources both in USCYBERCOM and NSA/CSS are probably funded via the NIP which is a Title 50 funding line led by the Director of National Intelligence (DNI).[13] Dual-hatting DIRNSA and Commander of USCYBERCOM could inhibit the maturation, growth, and development of service cyber components subordinate to USCYBERCOM due to the prevalence of NIP billets in both organizations. GEN Alexander could find himself forced to choose how to best use his human resources when he is constrained by law in the use of his Title 50 personnel funded via the NIP in that he must follow the DNI's priorities within the National Intelligence Priority Framework (NIPF) when allocating his NIP resources.[14]

RECOMMENDATION

1. To eliminate the conflict of interest created by giving one person the responsibilities of USCYBERCOM Commander and DIRNSA, USCYBERCOM should be elevated to the status of a functional unified command with a four-star officer in command and DIRNSA should be a separate three-star officer directing the CSA responsibilities supporting all unified commands as well as the POTUS, SecDef, other national decision makers, and the entire USG.

2. By separating these two positions, the Commander of USCYBERCOM can focus solely on Title 10 roles and responsibilities while identifying his/her priority intelligence requirements for

the U.S. Intelligence Community (IC) to answer as required.[15] Similarly, the DIRNSA could focus entirely on his/her Title 50 intelligence operations rather than military planning and operations that fall within the Title 10 realm. This provides unity of command for both organizations while removing the inherent conflict of interest created by putting one person over both a CSA and a sub-unified command.

3. Separating DIRNSA from his USCYBERCOM command responsibilities restores a level playing field where all COCOM priorities can be weighed against each other as well as national priorities when DIRNSA must apportion resources against competing requirements according to NIPF priorities.[16] The Commander of USCYBERCOM would present his/her intelligence needs, just like all the other COCOM commanders, to DIRNSA to satisfy. This solution eliminates the awkward situation that exists today where GEN Alexander is presenting all of his USCYBERCOM intelligence requirements to himself as DIRNSA.

4. Finally, separating the two positions removes the temptation that currently exists for the Commander USCYBERCOM to inappropriately use Title 50 NIP funded billets to fulfill responsibilities that are primarily Title 10 in nature. This action would also serve as a forcing function for the services to properly plan and program for billets to source their respective cyber component forces in support of USCYBERCOM's Title 10 mission. Today, the lines can quickly blur when one tries to evaluate whether or not a billet is primarily supporting a Title 10 or 50 mission set.

COUNTERARGUMENT

1. General and flag officers are perfectly capable of wearing multiple hats and effectively balancing the potentially divergent and competing responsibilities. For example, according to Air Force doctrine, the Joint Force Component Commander will usually fill roles as the Airspace Control Authority, Area Air Defense Commander, and Space Control Authority.[17] At the COCOM level of responsibility, dual-hatting works with the same officer serving as Commander, U.S. Northern Command (USNORTHCOM) and North American Aerospace Defense Command (NORAD), and another officer serving as Commander, U.S. European Command (USEUCOM) and Supreme Headquarters Allied Powers Europe (SHAPE). Both the NORAD/USNORTHCOM and SHAPE/USEUCOM commanders are responsible for a multinational combined command in addition to their COCOM command responsibilities. However, there is no fundamental conflict of interest inherent in dual-hatting these positions compared to that of DIRNSA and USCYBERCOM. In both examples, the combined command responsibilities correspond to the Area of Responsibility (AOR) assigned to their COCOM. Both USCYBERCOM and NSA/CSS have a global AOR but have the added tension of providing a supporting relationship to other COCOMS along with the inherent difference between operational missions of military operations versus intelligence operations.[18]

2. Warfare in cyberspace is intrinsically linked to cyber intelligence and requires a special relationship between the NSA/CSS and USCYBERCOM.[19] In order to ensure that USCYBERCOM receives the specialized intelligence required to enable mission accomplishment which in turn supports all the other COCOMs, the USCYBERCOM Commander should be the same person as the DIRNSA. While this argument seems sound on

the surface, it fails to see the fundamental conflict of interest created by combining the responsibilities of a COCOM commander with a CSA. CSAs must balance and prioritize requests from all the COCOMs[20] as well as national decision makers starting with the POTUS. While COCOMs will be directed to serve in "supported" and "supporting" relationships with each other,[21] CSAs have a broader customer set beyond the COCOMs. For example, U.S. Special Operations Command (USSOCOM) is extremely reliant on tailored intelligence to accomplish its missions but does not require direct control of any CSA to receive that required intelligence support. In fact, the other COCOM commanders would rightly object if USSOCOM proposed that their commander should also command a CSA such as the Defense Intelligence Agency (DIA) or the National Geospatial-Intelligence Agency (NGA) due to USSOCOM's special relationship with and/or reliance upon DIA or NGA. Obviously, all COCOMs as well as other national customers rely on CSAs to answer their priority intelligence questions, especially during Phase 0 shaping operations.

3. The cyber defensive expertise in NSA's Information Assurance Directorate (IAD) is essential to USCYBERCOM's success. This is a true statement. However, IAD's services are foundational for all the services and COCOMs not just USCYBERCOM. One could just as easily assert that the cyber defensive expertise in NSA's IAD is essential and foundational to all the COCOMs' and military services' successes in cyberspace operations.[22] While USCYERCOM will certainly leverage the unique expertise found in NSA's IAD, theirs is not an exclusive requirement that negates the needs of the other COCOMs and military departments for IAD's unique skill set.

CONCLUSION

Due to the inherent differences in the goals of military and intelligence operations, the conflict of interest in having the same person as a customer to himself, and the funding of human resources by NIP dollars in a fiscally constrained environment, DOD needs to separate the Commander, USCYBERCOM position from the DIRNSA position and appoint two different people to lead the respective missions of those two organizations. While general and flag officers are certainly capable of wearing multiple hats, there is a fundamental problem with combining a COCOM with a CSA since all CSAs must support a national-level customer set (including the POTUS) as well as all the COCOMs and military departments. Focusing on the NSA/CSS information assurance expertise highlights the need for an independent DIRNSA who can prioritize efforts within the NSA/CSS to meet competing requirements across their entire customer set of the USG not just the COCOMs or a single COCOM such as USCYBERCOM. The evidence clearly points to the best course of action—separate the position of Commander of USCYBERCOM from the Director of NSA to ensure successful mission accomplishment by both organizations.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. National Security Agency/Central Security Service, "Biography—Commander, U.S. Cyber Command, Director, National Security Agency/Chief, Central Security Service," http://www.nsa.gov/about/leadership/bio_alexander.shtml
2. Ibid.

3. Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*,5 January 2012, II-16.
4. Ibid.
5. President's Budget FY13, 85.
6. NSA/CSS, "FAQs About NSA", #10.
7. SecDef, *National Military Strategy for Cyberspace Operations*, December 2006, A-1.
8. JP 3-0, *Joint* Operations, 11 August 2011, V-8.
9. ODNI, *The National Intelligence Strategy*, August 2009, 2-3.
10. JP 2-01, II-16.
11. ODNI, *The National Intelligence Strategy*, August 2009, 5.
12. Richard Kogan, Center on Budget and Policy Priorities, "How the Across-the-Board Cuts in the Budget Control Act Will Work," Part 2, http://www.cbpp.org/cms/?fa=view&id=3635
13. ODNI, *The National Intelligence Strategy*, Forward.
14. JP 2-01, III-13.
15. Ibid., II-2.
16. Ibid., III-13.
17. Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011, 92.
18. NSA/CSS, "FAQs About NSA", #10.
19. AFDD 1, 46.
20. JP 1-02, *Department of Defense Dictionary of Military and Associated* Terms, 8 November 2010 (As Amended Through 15 March 2012), 58.
21. JP 3-0, III-5.
22. NSA/CSS, "FAQs About NSA", #5.

BIBLIOGRAPHY

Kogan, Richard. Center on Budget and Policy Priorities, "How the Across-the-Board Cuts in the Budget Control Act Will Work," Revised April 27, 2012, Part 2, http://www.cbpp.org/cms/?fa=view&id=3635

National Security Agency/Central Security Service, "Biography—Commander, U.S. Cyber Command, Director, National Security Agency/Chief, Central Security Service," http://www.nsa.gov/about/leadership/bio_alexander.shtml

National Security Agency/Central Security Service, "Frequently Asked Questions About NSA," http://www.nsa.gov/about/faqs/about_nsa.shtml

U.S. Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated* Terms, 8 November 2010 (As Amended Through 15 March 2012).

U.S. Department of Defense, Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, 5 January 2012.

U.S. Department of Defense, Joint Publication 3-0, *Joint Operations*, 11 August 2011.

U.S. Department of the Air Force, Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011.

U.S. Office of the Director of National Intelligence, *The National Intelligence Strategy*, August 2009.

U.S. Office of the President of the United States, *The Budget for Fiscal Year 2013*, February 13, 2012, http://www.gpo.gov/fdsys/pkg/BUDGET-2013- BUD/pdf/BUDGET-2013-BUD-8.pdf

U.S. Office of the Secretary of Defense, *National Military Strategy for Cyberspace Operations*, December 2006.

Integration of the Joint Cyber Center Organization Construct for Implementing SECDEF's Transition CONOPS for Cyberspace C2

Major Gabrielle J. Bryant-Butler, U.S. Air Force (USCENTCOM/J6)

ABSTRACT

As we continue to grow in the field of Cyberspace our transformation demands our senior leadership formalize a construct for integrating Cyberspace into every facet of our military organizations. On 30 Jan 2012, the Joint Chiefs of Staff (JCS) Tank approved the C2 Transition CONOPS. This plan states Combatant Commands (CCMDs) must activate a JCC with an expected activation date NLT 20 Apr 2012. Understanding the global nature of cyberspace and the necessity for standardized planning and execution, this concept takes into consideration CCMD, Service, and Agency requirements with their existing roles and responsibilities and allows CCMDs to use current authorities to generate effects in a timely manner. While the interim framework is in use, the intent is to capture lessons and make recommendations to the Joint Staff to improve the C2 framework eventually resulting in an enduring cyber C2 architecture. The JCC ultimately will be designated the backbone for command cyberspace operations, including DOD GIG Ops (DGO), Defensive Computer Ops (DCO), and Offensive Computer Operations (OCO).

DESCRIPTION OF ISSUE

1. One of the greatest issues facing our military today in the wake of Cyber advancement is how to leverage effective C2 in achieving unity of effort in this domain. Our leaders have come to realize continual, integration among the CCMDs, Services, and Agencies undoubtedly will be necessary to our success. A standard approach is more desirable as we consider the diverse mixture of forces involved: those native to tactical maneuver units; some theater forces; Service global forces; Service cyber commands assigned to USSTRATCOM; and other theater and global cyberspace support agencies.

2. Currently, coordination of cyberspace operations is managed through disjointed systems and complicated staff procedures. Clarke stated, "if (our) own military is mired in the ways of the past, overcome by inertia, overconfident in the weapons we have grown to love and consider supreme. The originator of the new offensive weaponry may be the loser unless it has also figured out how to defend against the weapon it has shown to the rest of the world."[1] Our military cyberspace is not comprised of any single network. It is a conglomeration of NIPRNET, SIPRNET, and an improvised combination of tactical and other networks managed by the four Services, the CCMDs, and multiple DOD agencies. In this present state no Geographic or Functional CCDR can control or defend their networks adequately in this new cyber era. Additionally, "as the scale of cyber warfare's threat to U.S. national security and the U.S. economy has come into view, the Pentagon has built layered and robust defenses around these military networks and inaugurated USCYBERCOM to integrate cyber defense operations across the military."[2] However, "more work is needed."[8] Despite cyberspace's critical role, we currently lack a standard approach to cyberspace C2, potentially reducing operational effectiveness, especially during times of crisis.

3. Over the past 10 years, the frequency and sophistication of intrusions into U.S. military networks have increased exponentially. Every day, U.S. military and civilian networks are probed thousands of times and scanned millions of times.[3] Many of the DOD functions,

including C2, are critically reliant on secure access to accurate information and trusted communications systems. Our adversaries undeniably have demonstrated the ability at infiltrating DOD systems and exploiting information. The frequency, with which adversaries could exploit vulnerabilities in the DOD GIG, jeopardizes our capacity to perform key military operations. Our reliance on cyberspace accelerates and increases risk, with the probability of our adversaries to gain an operational advantage. By holding our communications systems and information nodes at risk, the threat to disrupt our decision cycle and our ability to support operations in all domains remains in jeopardy. An even more significant problem is the difficulty in detecting and measuring both the direct and indirect costs of these security risks.[4]

4. The preponderance of our warfighting leaders have voiced a requirement for a cyberspace concept that provides clear policies and procedures. Additionally, there remains a need for synchronization and integration across all three cyberspace lines of operations. As GEN Alexander stated before the House Committee on Armed Services these LOOs are to "direct the operations and defense of the Global Information Grid so the Department of Defense can perform its missions, stand ready to execute full spectrum cyber operations on command, and stay prepared to defend our nation's freedom of action in cyberspace. "[5] A required element of this concept is to recognize that cyberspace is also more than a functional area but a domain which we operate in to conduct missions which spans all of DOD. Effective C2 is critical to achieve this unity of effort across the cyberspace domain.

RECOMMENDATION

1. A standard approach is required to maximize effort across Cyber's broad spectrum. Partnership, collaboration, and cooperation amongst the CCMDs, Services, and Agencies, will be the key to success. Cyberspace has interconnected and global operating layers that must be concurrently understood and coordinated. Most cyberspace operations have the potential to cause instantaneous effects at global levels that make them trans-regional in nature and of interest to a larger operational community. Given the complexities and interdependencies within this domain, it is imperative that the cyberspace C2 framework be clear, concise and standardized.

2. Furthermore, we must understand that cyberspace is not a functional area, but instead a domain in which we conduct operational missions which spans all of DOD. Scherrer and Grund noted "some might claim that cyberspace is purely an enabler best viewed as a functional area. Even if this were true, the current command structure is not in accord with the nature of the domain. Even geographically based thinking is a poor attempt to delineate artificial C2 boundaries when the global nature of cyberspace argues against this approach."[6]

3. In addition to, we must promote partnership and cooperation that improves existing Cyber C2 and allows a more deliberate approach at achieving an enduring framework. Scherrer and Grund also stated "The correct military response lies in establishing a C2 structure for this new domain so that the Armed Forces can not only execute day-to-day defense but also fight through future intrusions in time of war."[6]

4. To be successful we must "integrate the theory of Command and Control, as well as situation awareness, into an operational system."[7] Upon SECDEF approval, CCDRs would

implement an interim C2 architecture for DOD Title-10 cyberspace operations using existing capabilities and personnel structure in order to standardize the cyber C2 architecture across the DOD. The size and structure of the JCC would be at the discretion of the CCDR. CCDRs have the inherent flexibility to shape the JCC to best support mission and AOR requirements, as long as the JCC is still capable of performing the tasks and conforms to the command relationships as stated. To help achieve the objectives set forth we must formalize the cyber C2 architecture across the DOD, integrate planning, execution, and facilitate the validation of a more enduring C2 architecture. CCMDs, through their JCC, supported by the CYBERCOM Support Element (CSE), will operate along the three cyberspace LOOs. They will integrate command, planning, operations, intelligence, targeting, and readiness processes. Additionally, in partnership with USSTRATCOM they will engage and coordinate regionally with interagency, and allied partners (as necessary).

COUNTERARGUMENT

5. In opposition to this construct one could disregard the call for partnership and allow each CCMD, Service and Agency to continue to be responsible for their selective "foothold" (Intel in the "2" for exploit of cyber threats and analysis, Ops in the "3" for active cyber operations, and Communications in the "6" for the provide and the defense of cyberspace). We would persist in employing the respective subject matter experts in each specialty to analyze and respond based on their functional needs. As we continue to hold the mantra true "do more with less," today we're facing a new Cold War with China, while at the same time we are cutting spending and reducing troop strength.[8] An additional suborganization will only drain already limited manpower and personnel allocations and regardless of the new umbrella the respective representatives will simply revert back to their professionally trained opinion and ultimately their selective interests.

6. Additionally, one could argue to rely solely on USCYBERCOM to provide the necessary defense as required. USCYBERCOM has been established to:

> Fuse the Department's full spectrum of cyberspace operations and plan, coordinate, integrate, synchronize, and conduct activities to: lead day-to-day defense and protection of DOD information networks; coordinate DOD operations providing support to military missions; etc…"[9]

Accordingly, USCYBERCOM has been granted the mantle to improve DOD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and guarantee access to cyberspace."[9] With four service elements to include: USA – Army Forces Cyber Command (ARFORCYBER), USAF – U.S. Air Force, 24th Air Force, USN – Fleet Cyber Command (FLTCYBERCOM) and USMC – Marine Forces Cyber Command (MARFORCYBER). The responsibility remains with this organization to bolster our network and cyber defenses.

CONCLUSION

7. In conclusion, we are witness to "cyberspace emerging as the fifth domain of warfare and a crucial operational concern. As such, it requires a C2 system that enables defensive and operational capabilities within cyberspace."[10] Based on our ever growing mission set, our best interest is to reorganize existing CCMDs cyberspace coordination organizations and applicable staff elements into a JCC using a standardized cyberspace C2 model and integrate all facets as

required. Synchronize actions across a global domain and within geographic and functional areas of responsibility. As ADM Mullen stated before the 112th Congress:

> "We must devote the same time and attention to cultivating this nation's cadre of future cyber warriors as we do to our combat specialists. We must also empower Cyber Command and the combatant commands by working with the Executive Office of the President and other agencies to develop appropriate cyber authorities and by refining our cyber doctrine, tactics, and procedures."[11]

How do we best achieve this? By establishing an "interim framework" C2 model that improves existing Cyber C2 mechanics and allows a more studied approach at achieving an enduring and uniform C2 architecture that defines global, regional, and functional cyberspace operational lanes; enables unity of effort; and allows CCMDs to use current authorities to generate effects in a timely manner. While the interim framework is in use, capture lessons and make recommendations to the Joint Staff to improve the C2 framework. The JCC and CSE, collocated at each CCMD, will work towards the common goal of effective and efficient planning, allocation and synchronization of cyber effects in three cyberspace LOOs with the CCDR's campaign plans and operations while maximizing unity of effort. As such, the JCC and CSE, leveraging USCYBERCOM capacity, will integrate cyber effects into plans, deconflict and synchronize supporting cyber, and conduct operational assessments and readiness functions as specified. Within 12 months, the JS in coordination with the CCMDs, USCYBERCOM, Services and Agencies will complete a comprehensive review and assessment of the interim C2 architecture based on steady-state, exercise, and contingency operations and will report the result to an OPSDEPS Tank. The purpose of this Tank will be to propose a final objective cyber C2 framework that will be presented to a CJCS Tank for approval ultimately resulting in an enduring cyber C2 architecture.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Clarke, "Cyber War: The Next Threat to National Security and What to Do About it", p.14
2. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," p.2
3. Ibid., p.1
4. Pfleeger and Rue, "Cybersecurity Economic Issues: Clearing the Path to Good Practice," p. 2.
5. Alexander, "Statement Before The House Committee on Armed Services," p.2
6. Scherrer and Grund, "A Cyberspace Command and Control Model," p.6
7. Onwubiko and Owens, "Situational Awareness in Computer Network Defense: Principles, Methods and Applications," p.43
8. Robinson, "Obama's Defense Cuts Mean More Mergers for Tech Investors" p.1
9. CYBERCOM Mission and Objectives p.1
10. Ruiz and Redmond, "A Military Doctrinal Perspective on Collaborative Situation Awareness and Decision Making," p.3
11. Mullen, "Posture Statement of Admiral Michael G. Mullen, USN, Chairman of the Joint Chiefs of Staff Before the 112th Congress," p.8.

BIBLIOGRAPHY

Alexander, Keith GEN. "Statement Before The House Committee on Armed Services," 23 Sep 2010. http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf

Clarke, R. *Cyber War: The Next Threat to National Security and What to Do About It.* (Harper Collins, 2010).

CYBERCOM Mission and Objectives. 2012. https://www.cybercom.mil/default.aspx

Lynn III, William. "Defending a New domain: The Pentagon's Cyberstrategy," Foreignaffairs.com, Sep/Oct 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new- domain

Social Media

Mr. (GS-14) Robert W. Bond, U.S. Air Force (USAFE/A6O)

ABSTRACT

In 2007, Department of Defense (DOD) made a policy decision to collaborate, participate, or to disseminate or gather information via DOD Internet services or Internet based Capabilities (IbC) but at the same time balance benefits and vulnerabilities. However, internet infrastructure, services, and technologies must be managed to mitigate risks to national security; to the safety, security, and privacy of personnel; and to Federal agencies. As a result, all Non-classified Internet Protocol Router Network (NIPRNet), shall be configured to provide access to IbC across all the DOD Components.[1] DOD was very clear that IbC capabilities shall not be used to collect, disseminate, store, or otherwise process non-public DOD information. This caveat then allowed DOD to not be subject to Federal or DOD information assurance standards, controls, or enforcement, and therefore may not consistently provide confidentiality. While DOD laid out the policy for use, what DOD has not done as part of their policy is lay the foundation for control and monitoring of this non-value added service for normal mission support. When DOD talks IbC capabilities, Social Networking sites must be included in this capability from a reference point. The opening of IbC is missing the true issue concerning IbC: Is the DOD less or more productive since the opening of IbC sites?

DESCRIPTION OF ISSUE

1. Directive-Type Memorandum 08-037[2] allowed for the opening of IbC capabilities to the entire DOD community. However, due to velocity that it was executed by the field three issues were not properly addressed: effective guidance on use of IbC, control of usage/monitoring of IbC traffic, and charge back or recouping of cost associated with excessive IbC use. Once more formal guidance was solidified with DODDI 8550.01 however; the issues were still not addressed to a point where they were actionable.

When AFI 33-111 *"Telephone Systems Management"* existed, it clearly laid out guidelines for use of voice services. Paragraph 5, "Personal Calls over Official Telephones", states very clearly on what the phone service could be used for with regards to personal calls: "Commanders and supervisors may allow personal calls during work hours using official telephones if:

- The telephone call does not interfere with official duties
- The calls do not exceed reasonable duration and frequency, and whenever possible, are made during the employee's personal time such as after-duty hours or lunch periods
- The telephone calls serve a legitimate public interest (such as usage reduces time away from the work area or improves unit morale)
- The telephone call does not reflect adversely on DOD or the Air Force
- The government does not incur any long distance or per-call charges beyond normal local charges. Determine normal local charges based upon historical averages."[3]

As we advanced through technology, we became less able or willing to set standards concerning use of IbC and even less willing to enforce those nebulous standards pertaining to IbC. Within the DODDI 8550.01, "Authorized users of unclassified DOD networks shall comply with all

laws, policies, regulations, and guidance concerning communication and the appropriate control of DOD information referenced throughout this Instruction regardless of the technology used."[4] It pushes the responsibilities to the components versus taking a position on the control or monitoring of IbC.

2. All Air Force bases have Blue Coat Proxy servers filtering all web traffic leaving their location. These Blue Coat proxy servers at Ramstein AB during a three month period from 22 November 2012 to 20 February 2013 recorded 7.2 years work of IbC traffic and 4.5 years worth of Social Networking traffic. Figure 1 shows both these data points to include other categories that Blue Coat generates.

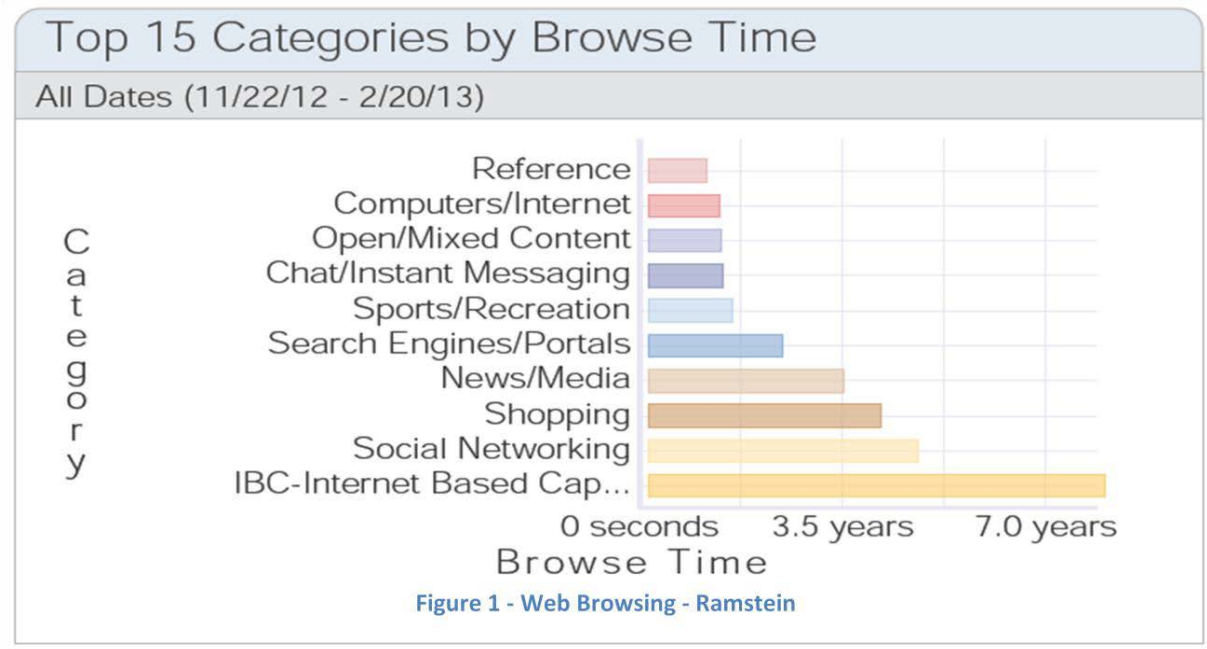

Figure 1 Web browsing at Ramstein AB[5]

If you take IbC, Social Networking, and Shopping together, they trump the rest of the categories together. Granted, the Air Force does buy merchandise, but we do not have that many GPC card holders that would equate to 4 years of web traffic at Ramstein AB. Ramstein AB has approximately 12,500 active user accounts, which includes many locations within the local area known as the Kaiserslautern Military Community (KMC). If we assume that Social Networking and IbC are mutually exclusive categories with no interaction then the KMC had 11.7 years of web browsing in only a three month window. If you break this down, it equates to 8.2 hours of web traffic per person per day during those 90 days. From purely an 8 hour work day perspective, surfing the web for 8.2 hours per day would lead the reader to believe that the data is wrong but never the less it is a data point that is worth further discussion. For example, let us assume that if an individual has four browser windows (e.g. Internet Explorer) open viewing four different IbC pages then that individual's viewing time is four times that of someone with only one IE window open. This could easily explain why there are over eight hours of web

browsing per person per day. Let us look a little further at some of the specific sites that continue this thread due to a lack of control with Ramstein's top 5 web sites. In order, starting with the most hits is FaceBook, some combination of RamsteinYardSales (must be at Ramstein to understand), some combination of Google, and finally YouTube. Of those five sites, two of the top five sites are IbC sites with FaceBook in the lead with 38.3 days while YouTube is four with 6.5 days, see Figure 2. RamsteinYardSales, which has absolutely nothing to do with operations but is a huge mission support for those with Permanent Change of Station orders (PCS) in and out of Ramstein AB, was a close second with 31.1 days. While the mechanism exists for the monitoring of network traffic through Blue Coat, there is nothing that limits individual web surfing activity with the exception of prohibited and illegal sites. What exactly is the purpose of allowing this capability? Perhaps the reason is to make the government more transparent, or to allow better access to government data, or to allow the federal government to sponsor the largest Morale, Welfare, and Recreational network for its 3.2 million personnel. With these two examples it does beg the question, "What are these individuals doing for the federal government when they are web surfing?" In order for the average civil servant (those that are not furloughed) to do their job, very little is required from IbC in order to accomplish it, appendix 1 has a complete listing of IbC sites. Having interviewed the Chief Technology Officer for USAFE/A6, zero access to IbC is required to do 99% of the jobs within USAFE. We have allowed people to do their personal business on a government network with zero controls.

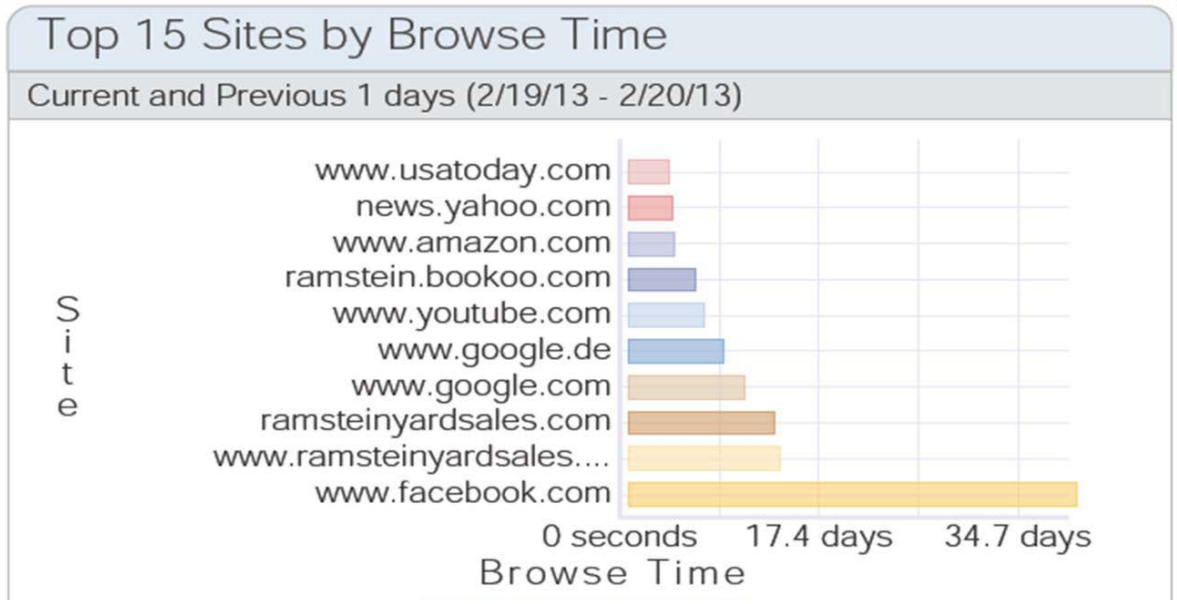

Figure 2. Top 15 sites at Ramstein AB[6]

3. As new technology is introduced into our society, we have always had mechanisms or methods to ensure the careful use and payment for the service. Let us start with standard analog phone service. In the late 1990's, commercial telephone connectivity gave us enormous capability for reaching across the whole world but at the same time, creating a time-consuming process to ensure the actual customer was paying for the service. Over time, the communications community has ensured that the rightful users of those charges were paying for incurred charges.

Moving ahead to cellular communications, it is very easy to determine who owns a particular device based on who is paying the bill. In both of these examples, the biggest issue for many of the communication units is the basic question, "Were these charges in performance of official duties?" For both of these, organizations used their Telephone Control Officer to go back to unit personnel to verify that they were "For Official Use Only" and if they were not, the individual members were required to reimburse the federal government. When the federal government implements mainstream activities that are commonplace in industry, things tend to be implemented differently than the industry for one primary reason, United States Government is a not-for-profit organization. Take Microsoft or Cisco, two top industry leaders within the communications industry, both for profit organization with a charge back system for providing network services for its departments. Each department within their company is charged an informational technology expense that must be covered by the business department as part of its operations. The federal government and particularly the Air Force see all network services as a core service or utility like water, electricity, and heating. Over a long period of time, dial tone for phone service has been seen that way as well, now network services are becoming a utility service to include web browsing. The federal government is looking at network costs as a sunk cost or perceived as no cost to the average DOD employee. As a result, everyone takes network services for granted and assumes the service will always be there and remain free to the users. But there is an actual real cost and there is also a hidden cost: productivity.

RECOMMENDATION

1. There are valid web browsing needs within the DOD and the Air Force for IbC services like Public Affairs, Chaplain Service, and the Intelligence community to include senior leader engagements particularly from a USAFE or PACAF standpoint. Existing Air Force guidance for providing internet resources to employees is defined as, "The Air Force goal, within acceptable risk levels, is to provide personnel requiring access for official business maximum accessibility to Internet resources."[7] The key part of the definition is for official business. However, the guidance on how we will use that Internet service is defined as "users must be disciplined in the quantity and content of non-mission essential information provided via Air Force networks".[8] In addition to that very generic statement, DOD states that components will, "Educate and train subordinate DOD employees in the responsible and effective us of DOD Internet services and IbC."[9] As a result of the Air Force trying to reduce the number of Air Force Instructions (AFIs) they have gone away from prescriptive AFI's to more generic content that assumes the average user is responsible. The data provided in figures 1 and 3 indicate that IbC traffic from Ramstein personnel are anything but responsible. AFI 33-129, *Web Management and Internet Use*, needs to be updated to be more prescriptive, similar to AFI 33-111. The guidance needs to explain exactly how and when this is to be used; with the technology evolution, this is no different than the phone system in the 1990's whose use was very prescriptive in AFI 33-111.

2. Appendix 1 has 122 web sites that are not needed for mission support for 99% of the Air Force population with the exception of those noted in the preceding paragraph. One of the hidden reasons for opening IbC in the first place was to allow our deployed armed forces to be able to contact their family members and loved ones in order to allow them to be more connected. No one will argue this point with anyone. As shown by figure 1 and 2, the Air Force has the ability to monitor our web traffic activity. The Air Force needs to control and throttle their web traffic. One option available for this is to restrict CONUS and garrison based OCONUS units access to IbC sites but allow access for CENTCOM's, SOUTHCOM's, and

AFRICOM's deployed locations. We also have the capability, at no cost to the government, to allow full access for those organizations needing it for operations while at the same time restricting it for the average DOD and USAF employee. Giving full access to all and hope they will not abuse it is not working as shown by the two figures above. You could potentially establish a Security Group within active directory that would either restrict or limit based on the amount of data transferred via the web. By creating a real-time throttle per category one could eliminate the issue we had two years with March Madness 2011, where everyone was streaming the basketball games to their local desktop.

3. Taking our last recommendation a step further into a charge back system, if our networks have become a commodity, then let us treat them as such and charge the users for the service. Taking a look at commercial cellular providers who do this very thing today with standard monthly cellular plans, there can be a limit on the data portion of your plan. Let us say you have an unlimited data plan up to 5gigabyte (GB) per month. After that, there will be a charge for every GB or portion of GB after that per month allocation. This technology exists today to implement this restrictive strategy but would need to be modified so that when personnel hit a certain limit on IbC traffic their access to IbC sites will be terminated until the following month or a cost is charged back to the user's unit. As noted in the previous paragraph, there are exceptions to this policy for those that need it like Public Affairs, Intelligence, and Religious communities. With the hardware and software already owned and operated by the Air Force, implementing this adds zero additional cost to the Air Force. There will be costs to ensure the system is implemented properly but it can be done with existing resources and current manpower.

COUNTERARGUMENT

1. If indeed DOD is treating network services like a commodity, then why would they be charging for it today? Air Force personnel do not get charged for commodities today like water, electricity, sewer, and heating. It is the Civil Engineers responsibility to pay the bill regardless of how much the base personnel use. Now granted, in the past few years the Air Force has been on a power conservation initiative to try and reduce the demand on our limited resources, but at the end of the day the Civil Engineers are still responsible for paying the base's bill. The one difference with the network service commodity is that if base personnel use 1GB or 5 GB worth of data it is exactly the same price. And if that was the case, then there should not be any throttling or restricting of web services for a core service that is provided as a result of the communication squadron for the betterment of the operational mission and its personnel. It is not as if the Air Force is limiting NIPRNet services; unless you are at a very small geographic separated unit. However, most main operating bases have plenty of capacity for web service traffic.

2. The next logical thought pattern by those that would be limited or restricted all together would be, "Why would the government restrict my ability to surf the web if I am not harming anything?" What is the government trying to hide by not allowing me to surf the web? DOD has authorized this capability for all DOD employees, why is the Air Force not supporting the DOD initiative for more transparency in government?

3. The last position people could take is, "Yes, I have six IE windows open, but they are in the background and are not doing anything except when I get a few minutes to check my

webmail, Facebook, YouTube, or PhotoBucket." Personnel will state, "I only check it for about five minutes a day, but since I have all of them open the Proxy Server is tracking that I'm on the Internet for about 48 hours in a single day." That equates to about 48 hours of web browsing (e.g. 8 hours X 6 IE windows equals 48 hours).

CONCLUSION

1. The DOD has embraced it and continues to push for IbC as a means of releasing information that is publicly releasable. DOD has been doing this since July 5, 1967 with the creation of the Freedom of Information Act that was enacted in 1966. The only exception is the media. In the past you had to officially request for data. More recently however, much of that data is now available for the taking as long as you own a computer. IbC is not without its pitfalls. If Ramstein AB personnel are viewing 7.2 years of work in IbC traffic in a three month period what is the Air Force or DOD viewing across an entire year. What is the unrealized cost associated with it? The answer is most likely a considerable loss in productivity.

2. DOD is the single largest employer of civilians in the United States at roughly 880,000 and has a total population of approximately 3.2 million personnel (2012).[10]. Of those 880,000, 370,000 are Air Force Civilians supporting operations around the world which would equate to 213 years' worth of browsing in a three month period. If civilians are surfing 213 years' worth of web traffic in only three months, what mission is not being accomplished? In these times of reductions and shrinking resources, we need every person doing the job they have been hired for, not surfing the web checking their Facebook account. Since the activation of IbC, this capability has been deemed a core service for both federal civilians and the military population. IbC is here to stay but will need to have a system developed to control use and a charge back system to ensure self-regulation of IbC in these fiscally trying times.

REFERENCES

1. Department of Defense Instruct ions (DODI) 8550.01. DOD Internet Services and Internet-Based Capabilities, 11 Sep 2012.
2. England, Gordan Under Secretary of Defense. To Secretaries of Military Departments. Policy for Department of Defense Interactive Internet Activities (DTM 08-037), 8 Jun 2007.
3. Air Force Instructions 33-111. Telephone Systems Management, 1 June 2001.
4. Department of Defense Instruct ions (DODI) 8550.01. DOD Internet Services and Internet-Based Capabilities, 11 Sep 2012.
5. Bluecoat Report 9.2. USAFE Bluecoat Proxy Traffic. (Accessed 20 Feb 2013).
6. Bluecoat Report 9.2. USAFE Bluecoat Proxy Traffic. (Accessed 20 Feb 2013).
7. Air Force Instructions 33-129. Web Management and Internet Use, 18 November 2008. Section 2.0
8. Air Force Instructions 33-129. Web Management and Internet Use, 18 November 2008. Section 6.8
9. Department of Defense Instruct ions (DODI) 8550.01. DOD Internet Services and Internet-Based Capabilities, 11 Sep 2012.
10. Alexander, Ruth. "Which is the world's biggest employer?" BBC News Magazine, 20 Mar 12. http://www.bbc.co.uk/news/magazine-17429786

Appendix 1
(Internet Sites within the IbC Category)

addthis.com	aolcdn.com	athlinks.com	bellwebcasting.ca
blackplanet.com	blogger.com	cafemom.com	cakefinancial.com
care2.com	changepass.stisecure.com	chat.aim.com	classmates.com
comcast.net/webmail	compasswhmc.stisecure.com	dailybooth.com	enrollpass.stisecure.com
facebook.com	fbcdn.net	flickr.com	foursquare.com
friendfeed.com	friendster.com	google.com/analytics	google.com/images
google.com/moderator	gotomeeting.com	groups.google.com	hi5.com
hotmail.com	images.google.com	imgur.com	linkedin.com
live.com	live365.com	livejournal.com	login.yahoo.com
mail.aol.com	mail.google.com	mail.yahoo.com	mcstatic.com
meetup.com	metacafe.com	moveable.com	moveableonline.com
moveabletype.com	moveabletype.org	mtv.com	mybcdna.com
myspace.com	myspacecdn.com	myworkster.com	myyearbook.com
opendiary.com	orkut.com	pbsrc.com	photobucket.com
plaxo.com	safeweb.norton.com	screenname.aol.com	siteadvisor.com
sitereviewer.com	slideshare.net	socialtext.com	socialvibe.com
staticflickr.com	stumbleupon.com	stumble-upon.com	togetherweserved.com
twimg.com	twitter.com	webmail.aol.com	webmail.att.net
webmail.austin.rr.com	webmail.bak.rr.com	webmail.bham.rr.com	webmail.ca.rr.com
webmail.cfl.rr.com	webmail.cox.net	webmail.east.cox.net	webmail.ec.rr.com
webmail.elmore.rr.com	webmail.elp.rr.com	webmail.eufaula.rr.com	webmail.gt.rr.com
webmail.hawaii.rr.com	webmail.houston.rr.com	webmail.hvc.rr.com	webmail.insight.rr.com
webmail.jam.rr.com	webmail.kc.rr.com	webmail.ma.rr.com	webmail.mass.rr.com
webmail.mi.rr.com	webmail.nc.rr.com	webmail.neo.rr.com	webmail.new.rr.com
webmail.nj.rr.com	webmail.nyc.rr.com	webmail.panhandle.rr.com	webmail.roadrunner.com
webmail.rochester.rr.com	webmail.satx.rr.com	webmail.stny.rr.com	webmail.stx.rr.com
webmail.sw.rr.com	webmail.tampabay.rr.com	webmail.tx.rr.com	webmail.verizon.net
webmail.west.cox.net	webmail.woh.rr.com	webtac.ugs.com/logir/	weourfamily.com
wordpress.com	wordpress.org	xanga.com	yammer.com
yimg.com	ustream.tv	vimeo.com	trooptube.tv
youtube.com	ytimg.com		

Cyber Attack Policy: How to Ensure a Cyber Attack Policy is Just, Legal, Resources, and Appropriately Led

Lt Col Michelle C. Carns, U.S. Air Force (338 TRS/CC)

ABSTRACT

Multiple methods of cyber attack exist in various permutations which could be characterized in familiar terms as covert action, pre-emption or a simultaneous combination of cyber and kinetic engagement.[1] In spite of the magnitude of the existential threat, comprehensive national and international laws and policy do not exist to defend and protect national centers of gravity in a legal and justified way due to various issues to include ideological conflicts and lack of prioritization[2] (but could be successful at least internationally if designed to be mutually beneficial[3]). Although complete policy does not exist either in the U.S. or internationally, U.S. national guidance indicates consistently documented national priorities, such as critical infrastructure, that would provide a foundation for justifying future cyber attack policy for decision makers that is legally supportable. This paper will briefly examine the widely-reported case of Stuxnet as a means to illustrate a cyber attack method, how a cyber attack can support policy, and yet that *the effect* may not be legal or justified, highlighting the importance of sound policy. Additionally, this assessment will recommend the policymaker for Cyber be moved up from Deputy Assistant Secretary of Defense (DASD, under Global Strategic Affairs) to an Assistant Secretary of Defense level (an "ASD-Policy" or "ASD-P" for Cyber) in the spirit of President Obama's *Cyberspace Policy Review* near-term action plan recommendation as noted in Table 1.[4] In addition, the ASD-P should be assigned resources via the Major Force Program (MFP) model (in the case of cyber, it would be number "13").[5]

DESCRIPTION OF ISSUE

1. In spite of the existential threat that cyber attack poses, comprehensive cyber attack policy in the U.S. is not clearly articulated, although it should be.[6] Some policy elements do exist, but they are hidden in existing strategic documents.[7] Similarly, doctrine mistakes guidance such as "initiatives" calling them policy, for example, the recommendations found in the Comprehensive National Cybersecurity Initiative (CNCI).[8] Depending on circumstances and outcome, a computer attack initiated by an adversarial nation-state could constitute an "act of war" in which case national and international laws regarding self-defense could support a response.[9] In the case of an attack, any response would have to be based on policy "bounded" by laws supportive enough to enable any mission required. However, since many "attacks" that occur in cyberspace are actually crime and espionage, response may simply require adequate legal action (versus a nation-state kinetically responding to an attack) through media and public affirmation of attacks by another nation or entity.[10] Thus, although policy is not fully articulated, existing national guidance found in two presidential documents point towards three areas the U.S. has prioritized that, if threatened, indicate they are important enough to constitute grounds for some form of retaliatory cyber attack: the importance of America's critical infrastructure, preserving business innovation and the crucial element of U.S. economic prosperity. Importantly, cyber attack policy must articulate those thresholds beyond which the U.S. will not tolerate an attack on national priorities and should guide national decision making to respond to those threats in a legal and justified way. President Obama's Executive Order 13636 states that critical infrastructure must be protected and illustrates a key area that could justify a policy in which a cyber attack would be justified.[9] The order stipulates that it is the "policy of the United states to enhance the security and resilience of critical infrastructure" and to ensure that the cyber "environment" is preserved

while observing privacy and laws.[11] From that standpoint, an attack on the security of the national cyber environment or critical infrastructure to the point of "incapacity or destruction" could be considered grounds for further action and a key policy element. Protection of critical infrastructure is echoed in *The National Strategy to Secure Cyberspace.*[12] Furthermore, *The International Strategy for Cyberspace* (May 2011) states that it is in the interest of our national strategy to support international policy that prioritizes innovation.[13] One could conclude that theft of intellectual property and repeated breaches of the banking industry as well as foreign probing of U.S. infrastructure constitute threats which disempower innovation. Recent public releases of information indicate that a cyber attack may be met with a media response as part of the retaliation portfolio. The White House confronted China publicly calling for the Chinese government to "stop the widespread theft of data" which alluded to the role of the Chinese military in attacking U.S. government agencies and companies on an ongoing basis.[14] Although China denied involvement, publishing supportable attribution of the attack source would be a justified means of retaliation. President Obama also prioritizes a "cyber environment" that ensures economic prosperity for the U.S. Attacks on financial institutions had destructive effects against American Express, JPMorgan Chase and others; although claimed by the online group Izz ad-Din al-Qassam Cyber Fighters, reporting indicates a possible connection to Iran.[15] Economic prosperity is clearly a priority and a significant enough threat against the security of the nation's economy indicates it is also a policy priority and a potential flashpoint that if put at risk, could trigger a cyber attack.

2. Cyber attack policy lacks legal guidance which is ultimately dependent on an accepted definition of what actually constitutes a cyber attack. Due to the proliferation of plausible definitions of cyber attack throughout current literature and doctrine, this paper will use the Joint Publication 3-0 *Joint Operations* definition which states that Computer Network Attack (CNA) "disrupts, denies, degrades, or destroys information resident in computers and computer networks (relying on the data stream to execute the attack), or the computers and networks themselves."[16] One of the limitations in this definition is that the U.S. has been subject to cyber espionage for many years and this definition doesn't articulate whether or not file theft from the Pentagon, for example, constitutes an attack or espionage. Without a clear definition, it is virtually impossible to properly identify an activity in cyber and then adequately prosecute the perpetrators. Espionage and criminal activities can be prosecuted as they would be under normal circumstances for such activities. However, legal parameters that identify triggers for addressing "the use of force" in cyber or an "act of war" in cyber have not been identified.[17] One analysis of applying legal concepts in cyberspace concludes that qualifying that a 'kinetic effect' against a target could constitute a way to bound the problem.[18] While traditional rules are still in effect for self-defense, pre-emption as a cyberspace attack method (as opposed to self-defense or retaliation after an initial attack) proves to be a unique challenge. The U.S. is allegedly currently reviewing the legality of a pre-emptive cyber strike.[19] The widely reported and analyzed case of "Stuxnet" and its impact to Iran's nuclear infrastructure illustrates the effect of a cyber attack and its resultant kinetic effect, but also shows the murky problem of whether or not that was a pre-emptive act which could have justified a declaration of war or retaliation. Stuxnet's attack on Iranian uranium centrifuges set back Iran's nuclear program, according to one report, from 18 months to 2 years.[20] If this was a targeted attack against Iran to destroy or hinder nuclear weapons development, as alleged by Iran, a pre-emptive attack against Iran's capability could be considered an illegal, pre-emptive cyber attack. Furthermore, if the criteria for cyber attack is for

a kinetic effect to occur, then Stuxnet would qualify, in which case if the attack could have been definitively attributed, Iran would have had the legal right to retaliate in self-defense.[21] Until laws clearly articulate the way ahead, cyber attack policy and its implementation will remain incomplete.

3. Cyber attack policy also lacks control of resources and the appropriate level of leadership to execute presidential directives for justifiable and effective action in support of national priorities. The existing Office of the Secretary of Defense policy advisor for cyber is a Deputy Assistant Secretary of Defense (under Global Strategic Affairs) which prevents proper authority level for "coordination and change" as directed by the President in Executive Order 13636.[22] Additionally, the Cyber DASD lacks the resources to effectively implement presidential directives. The importance of ensuring leadership and resources are adequately assigned to cyber cannot be underestimated.

RECOMMENDATION

1. Developing a single, comprehensive national policy document and utilizing existing strategic documents to form clearly articulated policy objectives, unique from initiatives and strategy, must be a priority to articulate and justify legal cyber attack. In order to effectively enact presidential guidance, the office of the existing policymaker for cyber should be moved up from Deputy Assistant Secretary of Defense (under Global Strategic Affairs) to an Assistant Secretary of Defense level (an "ASD-P for Cyber"). As an ASD for Cyber, the cyber policymaker would fall directly under executive authority, similar to a covert action as recommended in the CNCI.[23]

In a campaign speech, President Obama noted the importance of cybersecurity and stated he would, "appoint a National Cyber Advisor who will report directly to the President."[24] In order to effectively execute policy, the ASD-P for Cyber should also be assigned resources via the Major Force Program (MFP) model. Similar to the creation of MFP 11 for Special Operations Forces in 1987 in the Nunn-Cohen Amendment to the Goldwater-Nichols Act, and driven by several mission-related "imperatives,"[25] assigning resources to cyber would increase mission assurance in a contested domain. History records that Special Operations Forces were assigned MFP 11 only after a mission failure and loss of life.[26] It is essential that resources flow *proactively* to cyber in the form of a new MFP to protect critical infrastructure, ensure the protection of the financial and business sectors that fuel the U.S. economy, and provide for the general defense of the nation. In the case of cyber, the next MFP number available would make cyber MFP number "13".[27] Great Britain has an extremely effective model for unifying a policymaker with resources. Mr. John Taylor is the United Kingdom's (UK) Chief Information Officer (CIO) in the British Ministry of Defense. Such a proven precedent would ensure presidential policy is enacted in the cyberspace domain in a timely and effective manner.[28]

2. In order to sufficiently develop laws for Cyber, war in cyberspace must be adequately defined. Elements that constitute "war" in cyber should be established to guide policymakers and leaders in cyber attack operations that meet national needs for operating in cyberspace while ensuring freedom of movement in the cyber domain. Any laws proposed must meet the standard for *jus ad bellum* with respect to "necessity and proportionality."[29] Laws, rules of engagement,

policy and both national and international considerations can provide the "legal framework" for establishing appropriate cyber attack law.[30]

3. President Obama also prioritizes a "cyber environment" that ensures economic prosperity for the United States. Recent attacks on financial institutions had destructive effects against American Express, JPMorgan Chase and others. Although claimed by the online group Izz ad-Din al- Qassam Cyber Fighters, reporting indicates a possible connection to Iran.[31] Because whole-of government coordination and policy is only in the nascent stages, with respect to protecting the private sector through action, President Obama must incentivize his policy of voluntary reporting of cyber attacks and must ensure the private sector and government has access to a collaborative and timely means for reporting cyber attacks.[32]

COUNTERARGUMENT

1. Comprehensive cyber attack policy may not need to be created if the national leadership believes policy is already adequately and clearly expressed in various strategy documents and by executive order. Additionally, further policy articulation might constrain national action in cyberspace as the national leadership works through the constant challenges occurring in the cyber domain. Finally, if policy was developed prematurely, the U.S. might be at risk of being the only nation restricting themselves to particular actions related to cyberspace, in which case policy would be overly specific and incapable of ensuring an appropriate retaliatory response or action.

2. Cyber attack conducted in cyberspace may be impossible to regulate both nationally and internationally. For example, in the case of Stuxnet, regardless of origin, a pre-emptive, destructive attack may not have been a legal attack supportable by existing laws or may have constituted an "act of war" in which case Iran might have been legally justified in retaliating if they could definitively identify the source of the attack.

3. An ASD-P for Cyber is not required; the current level of cyber policymaker is appropriate to ensure cyber-related policy matures to meet advancing technology and adaptive adversaries. The existing level of cyber policymaker can currently provide sufficient presidential support. Cyber operations have not experienced a catastrophic mission failure in the way Special Operations Forces (SOF) did, which resulted in a loss of life. Desert One, the failed mission to rescue the hostages in Iran, which was a major driving factor for ensuring an MFP was assigned to SOF, has not occurred in the cyber realm.[33] The current resources structure is appropriate for cyber to operate effectively and efficiently. Assignment of an MFP would further confuse resources and lines of control in an already multi-faceted joint-force effort.

4. Finally, President Obama must incentivize his policy of voluntary reporting of cyber attacks by ensuring laws exist to protect the reporting organizations and their intellectual property. As a result, the private sector and government need access to a collaborative and timely resource for reporting cyber attacks such as a closed space like a restricted "range" where online collaboration and reporting can occur safely.

CONCLUSION

1. Complete cyber attack policy and associated laws must be established to protect the U.S. against cyber attack but must also enable U.S. freedom of action to respond to an attack against

crucial national elements such as critical infrastructure, innovation, and the economy. In spite of the magnitude of the existential threat, comprehensive national laws and policy do not exist to defend and protect national centers of gravity in a legal and justified way. Existing U.S. national guidance does indicate prevailing judgments that would justify either initiating cyber attack or in response to a cyber attack. These judgments can already provide a foundation for future policy that will ensure legally-sound decisions. Although some policy elements have been articulated, they are scattered throughout several key national documents and frequently appear as "initiatives," "strategies" or general guidance. These key policy points should be consolidated and lifted into a single, comprehensive policy document. As for the legal aspect of cyber attack, the case of Stuxnet illustrates the importance of ensuring U.S. laws recognize that depending on what type of cyber attack method is conducted, *the effect* of the attack may not be legal or justified, again highlighting the importance of sound and coherent policy. With the backing of Assistant Secretary of Defense (an "ASD-P" for Cyber) in the spirit of President Obama's *Cyberspace Policy Review* near-term action plan.[34] This ASD-P for Cyber should be assigned resources via the MFP model similar to the UK CIO model.[35] Cyber attack policy must also be supported by a secure reporting tool available to government and private entities to incentivize voluntary cyber attack reporting and to ensure all sectors have a means of identifying cyber attacks in a timely and collaborative way. With assigned resources and the appropriate level of the Office of the Secretary of Defense leadership, the U.S. can begin to enact executable and relevant cyber attack policy to support legally-justified operations in cyberspace, in order to meet President Obama's intent to remain the world's leader in protecting cyberspace and "assuring the future of the Internet itself".[36]

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* (Fall 2012): 64.
2. Robert Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* (Fall 2012): 20-21.
3. AFDD 3-12: 29.
4. President Barack Obama, *Cyberspace Policy Review*: *Assuring a Trusted and Resilient Information and Communications Infrastructure:* vi.
5. Stuart E. Johnson, "A New PPBS Process to Advance Transformation," *Defense Horizons*, September 2003, Number 32 and Maj Matt C. Hensley, USAF, Military Assistant to the Chief Informations Officer, Department of Defense interview by author on April 12, 2013.
6. President Barack Obama, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, May 2011.
7. Dr. John B. Sheldon, "Cyberpower and Strategy"(recorded lecture).
9. David E. Sanger and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *The New York Times*, May 31, 2011, retrieved from http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=0
10. President Barack Obama, *Cyberspace Policy Review*: 10.
11. Executive Order no. 13,636, *Improving Critical Infrastructure Cybersecurity*, title 3, p. 11,739.

12. *National Strategy to Secure Cyberspace*
13. President Barack Obama, *International Strategy for Cyberspace:* 3.
14. Mark Landler and David E. Sanger, "U.S. Demands China Block Cyberattacks and Agree to Rules, *The New York Times,* March 11, 2013, retrieved from http://www.nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set- cyber-rules.html?pagewanted=all&_r=0
15. Nicole Perlroth and David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times,* March 28, 2013, retrieved from http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html?pagewanted=all
16. Joint Publication 3-0: III-26.
17. Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, "The Law of Cyber-Attack," The California Law Review http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf , pp. 25-26.
18. Ibid., p. 26.
19. David E. Sanger and Thom Shanker, "Broad Powers Seen For Obama in Cyberstrikes," The New York Times, February 3, 2013, retrieved from http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?ref=stuxnet
20. Johnathan Fildes, "Stuxnet Worm "Targeted High Value Iranian Assets" BBC Online, September 23, 2010, retrieved from http://www.bbc.co.uk/news/technology-11388018 and David E. Sanger, "Obama Ordered Sped Up Wave of Cyberattacks Against Iran," retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks- against-iran.html?ref=stuxnet
21. Hathaway, Oona, et. al.: 5.
22. Executive Order no. 13,636, *Improving Critical Infrastructure Cybersecurity*, title 3, p. 11,739.
23. U.S. Congressional Research Service. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations (R40427; March 10, 2009) by John Rollins and Anna C. Henning.
24. Ibid, 24.
25. Col Maureen J. Smith, 81 TRG/CC, interview by author April 11, 2013 and Lt Col David E. Hill, Jr., USA, "The Shaft of the Spear: U.S. Special Operations Command, Funding Authority, and the Global War on Terrorism."
26. Lt Col David E. Hill, Jr., USA, "The Shaft of the Spear: US Special Operations Command, Funding, and the Global War on Terrorism": 20.
27. Stuart E. Johnson, "A New PPBS Process to Advance Transformation," *Defense Horizons* and Maj Matt C. Hensley, USAF, Military Assistant to the Chief Informations Officer, Department of Defense interview by author on April 12, 2013.
28. Maj Matt C. Hensley, USAF, Military Assistant to the Chief Informations Officer, Department of Defense interview by author on April 12, 2013.
29. Hathaway, Oona, et. al: 35.
30. AFDD 3-12: 34.
31. Nicole Perlroth and David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times,* March 28, 2013, retrieved from

http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html?pagewanted=all

32. President Barack Obama, Executive Order 13636: 11740.
33. Lt Col David E. Hill, Jr., USA, "The Shaft of the Spear: US Special Operations Command, Funding Authority, and the Global War on Terrorism": 20.
34. President Barack Obama, *Cyberspace Policy Review*.
35. Stuart E. Johnson, "A New PPBS Process to Advance Transformation" and Maj Matt C. Hensley, USAF, Military Assistant to the Chief Information Officer, Department of Defense interview by author on April 12, 2013.
36. President Barack Obama, *Cyberspace Policy Review*.

BIBLIOGRAPHY

Air Force Directive Document 3-12 (2010). *Cyberspace Operations*. Retrieved from http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf

Executive Order no. 13,636, *Improving Critical Infrastructure Cybersecurity*, title 3.

Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, "The Law of Cyber-Attack," The California Law Review http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

Hill, Lt Col David E., Jr., USA, "The Shaft of the Spear: US Special Operations Command, Funding Authority, and the Global War on Terrorism" retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA449333

Hurwitz, Roger. "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* (Fall 2012): 20-21, retrieved from http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf

Johnson, Stuart E., "A New PPBS Process to Advance Transformation," *Defense Horizons*, September 2003, Number 32, www.ndu.edu/CTNSP/docuploaded/dh32.pdf (accessed March 17, 2013).

Joint Publication 3-0, "Joint Operations," August 11, 2011.

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* (Fall 2012): 64, retrieved from http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf

National Strategy to Secure Cyberspace, http://www.dhs.gov/national-strategy-secure-cyberspace

President Barack Obama, *Cyberspace Policy Review*: *Assuring a Trusted and Resilient Information and Communications Infrastructure,* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

President Barack Obama, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Sheldon, Dr. John B., "Cyberpower and Strategy"(recorded lecture, Center for Cyberspace Research, Wright-Patterson Air Force Base, OH, April 10, 2013).

Smith, Col Maureen J., 81 TRG/CC, interview by author April 11, 2013.

U.S. Congressional Research Service. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations (R40427; March 10, 2009) by John Rollins and Anna C. Henning retrieved from Congressional Research Digital Collection (accessed March 15, 2013):17. See also the U.S. presidential response to the CNCI at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

ACKNOWLEDGEMENTS

Several individuals were instrumental in assisting the author to shape this Cyber DART to fulfill the requirements for Cyber 300 at the Air Force Institute of Technology. The author would like to recognize them as follows:

Annie I. Antón, PhD, Chair and Professor, School of Interactive Computing, Georgia Tech University. Dr. Anton was instrumental in talking the author through the wide variety of topics available to Cyber 300 students prior to course attendance. Through the course of discussion, Dr. Anton and the author agreed that the policy element may be among the most interesting and in need of examination. As a result, Dr. Anton guided the author to various sources to begin a literature review which helped the author scope down the general topic of "cyber attack" and "policy" into a focused discussion. Dr. Anton was also a gracious host to the author during the Georgia Tech Cyber Security Symposium March 28-29, 2013.

Professor Peter P. Swire, Esq., C. William O'Neill Professor of Law, Michael E. Moritz College of Law, Ohio State University. Professor Swire was instrumental in assisting the author to organize the structural flow of the cyber attack discussion in order to ensure the message was effectively and thoughtfully argued.

Stewart A. Baker, Esq., Partner, Steptoe & Johnson, LLP, was kind enough to field the author's questions following Mr. Baker's panel discussion during the Georgia Tech Cyber Security Symposium March 28-29, 2013. He also assisted the author in understanding some of the vast legal considerations which make the cyber domain so contentious.

Col Maureen J. Smith, 81st Training Group Commander, 81st Training Wing, Keesler AFB, Biloxi, Mississippi assisted the author in understanding strategic policymaking.

Maj Matt C. Hensley, Military Assistant to the Chief Information Officer for the Department of Defense, provided essential insight into the Chief Information Officer function in the United Kingdom. The author's interview with Maj Hensley provided precedence for linking policy and resources, which, prior to the author's discussion with Maj Hensley, was an idea without precedent. Maj Hensley was also aware of a "virtual" Major Force Program (MFP number 12) which the author did not come across in research and would not have been aware of otherwise.

PART V: NEW PARADIGMS

Establishing a Cyber Coordinating Authority within the Joint Command and Control Function
Major David T. Neuman, U.S. Air Force (92d Information Operations Squadron)

ABSTRACT

Cyber vulnerabilities within an interconnected operational environment require the addition of a Cyber Coordinating Authority (CCA) within the joint command and control function to ensure the unique space, time, and force characteristics of cyber capabilities do not become a decisive advantage for our adversaries. Commanders at the theater strategic and operational level derive essential support from the interconnected operational environment to achieve their objectives. The cyberspace domain threads together not only capabilities within the military establishment, but also critical government and civilian capabilities that enable military operations. In the past, cyber capabilities have been viewed as an enabling element. Today cyber power has emerged as a credible capability that can deliver effects in either a supporting or supported role to achieve tactical, operational or even strategic level objectives. This paper examines the unique characteristics of cyber capabilities and illustrates how vulnerabilities within the interconnected operational environment might be exploited by a competent cyber adversary to achieve an operational advantage over traditional U.S. military power. Finally, the paper proposes recommendations to address how best to instrument command and control capabilities in operations involving cyber warfare.

DESCRIPTION OF ISSUE

1. Commanders at the theater strategic and operational level derive essential support from the interconnected operational environment to achieve their objectives.[1] The cyberspace domain threads together not only nodes within the military establishment, but also critical government and civilian capabilities that enable military operations.

2. Dependence on cyberspace and the unique time, space, and force characteristics of cyber capabilities within an interconnected operational environment have created vulnerabilities that if exploited can seriously disrupt or neutralize operational functions such as protection, command and control, intelligence, fires, movement and maneuver, and sustainment. In that context, the unique characteristics of cyber capabilities are best explained when examined within the operational factors of time, space, and force. These factors are critical for the Joint Force Commander (JFC) who must carefully balance them when making decisions on how to employ forces against strategic and operational objectives. In the cyber domain these factors are highly dynamic and can affect the JFC's objectives far outside the geographic boundaries of his area of operation.

a. Cyber capabilities don't alter the concept of operational factors, but the unique characteristics pose significant challenges for commanders. For instance, cyber capabilities that shape computer and communication networks, transportation, and utility systems transcend the traditional features of ***factor space***. These capabilities are not constrained by geographic, political, economic or social boundaries or military movements we've known in previous conflicts; yet, they can have a decisive effect on military power. Capabilities in the cyber domain are projected across virtually any space without certain considerations such as host nation support for territorial basing of forces. In addition, because of the interconnected nature of some cyber based systems, employment of cyber capabilities in one geographic theater can have a direct impact in another. For example, a distributed denial of service attack on computer

systems at the New York Stock Exchange that prevents financial trading for even one day would have serious consequences across global financial markets. In the case of military operations, a similar type attack on Air Mobility Command's Tanker Airlift Control Center would degrade its ability to plan and execute tanker and airlift missions across all geographic commands. These space characteristics present a logical transition to consider the uniqueness of factor time.

b. The ***factor of time*** is the most critical and precious factor in the conduct of warfare.[2] Disadvantages of space and inferiority in forces can sometimes be remedied by acting faster and accomplishing the assigned objectives within a given period.[3] Unlike other instruments of war, most cyber capabilities move at near the speed of light – literally. This characteristic presents an adversary with the ability to engage an opponent at all levels of conflict and across an interconnected operational environment – military, political, economic, social, information, and infrastructure simultaneously. Additionally, although access to, and understanding of how cyber-based systems interface across an operational environment can take longer, the development of cyber tools and weapons can be developed and distributed or employed rapidly and at a very low cost. Another difference are cyber weapons can be covertly prepositioned prior to hostilities and "launched" in advance or in conjunction with kinetic capabilities once hostilities begin. While time may be the most critical factor, ***force*** perhaps presents the most challenging of the three operational factors.

c. Whether we are considering physical infrastructure networks, information networks, or cyber networks in today's environment, these networks and infrastructures are critical components of military power. It's not the rapidly evolving technology behind cyber capabilities that presents operational challenges, but the way we employ them. Milan Vego, a military operational art theorist, stated:

> Since the advent of the industrial era, even the most radical new technological advances, such as steam propulsion, the internal combustion engine, wireless radio, railways, submarines, aircraft, torpedoes, mines and missiles, were all successfully adopted by the militaries of the day. They all eventually resulted in significant increases in capabilities, which in turn led to changes in the methods of combat employment.[4]

Vego further theorized, these technologies were successful because they were adopted within the context of strategy, operational art, and tactics. Cyber capabilities and cyber technology should be considered in the same way. What we apply in military operations is not as important as how we apply it. Cyber capabilities cannot be considered a panacea that will negate the importance of other military capabilities or the art in how we apply them, but rather it must be a fully integrated part of operational planning to successfully achieve military objectives.

3. A growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy information. The continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the United States vulnerable to the loss of economic competitiveness and the loss of the *military's technological advantages*."[5] All technologies and strategies have vulnerabilities. What distinguishes vulnerabilities in the cyber domain is the interconnected nature of networks and the high degree of reliance U.S. private and public institutions place on the services provided by those networks. The military Global Information Grid[6] that supports

military operations in most cases uses the same common infrastructure, network systems, and software as commercial and private enterprises. It's not any one cyber system or network that presents the most serious vulnerability, but rather the totality of the cyber enterprise on which the U.S. and many other nations rely on for national security, economic prosperity, and basic societal and governmental functionality. In the strategy of a sophisticated adversary, cyber capabilities are not the end in themselves, but the means to achieve larger operational and strategic objectives. Complete examination of cyber vulnerabilities is too broad a subject area for this paper. Instead, a focus on the vulnerabilities in critical infrastructure and military operations provides the necessary analysis to understand the potential impact of a sophisticated cyber attack at the national strategic, theater strategic, and operational levels. Military planning and operations are intertwined with the nation's critical infrastructure. Understanding the vulnerabilities in these two areas will allow military leaders to plan for conflicts that include cyber attacks against systems underpinning our military strength.

4. Homeland Security Protection Directive (HSPD) 7 identifies 18 Critical Infrastructure and Key Resources (CIKR) sectors:[7] agriculture and food, banking and financing, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, healthcare and public health, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, transportation systems, and water. The focus of HSPD-7 is to protect CIKR against terrorist attacks. Furthermore, the National Infrastructure Protection Plan states, "Cybersecurity includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cyber security also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster."[8] What these directives fail to recognize is the potential for systematic, deliberate, and simultaneous attack and/or exploitation of cyber dependent systems and networks by a sophisticated adversary. It presumes a 9-11 like event that involves a handful of kinetic activities by a small group that cause mass effect. The lack of authority and ability to identify and respond to a deliberate and sophisticated cyber attack is in itself a vulnerability. Of the 18 CIKR sectors, there are 12 departments and agencies responsible for securing them.[9] The lack of authoritative structure is in part due to the fact that 85% of CIKR is privately owned and operated.[10] Civilian agencies are not alone in challenges pertaining to roles and responsibilities. In the event of a deliberate cyber attack on the U.S., the Department of Homeland Security (DHS) would be responsible for coordinating a response. U.S. Cyber Command under Strategic Command would provide DHS technical support, but it's still unclear how government and private organizations would tie together to neutralize the threat. Without clear lines of authority and responsibility to defend against and respond to complex cyber events, U.S. efforts would be cumbersome and perhaps ineffective. In an operational environment where salvos move at the speed of light these cumbersome and ineffective lines could provide an enemy a distinct advantage.

5. How do the time, space, force characteristics, and cyber vulnerabilities within an interconnected operational environment relate to the projection of military power? The answer is both directly and indirectly. There are also specific vulnerabilities within CIKR that can affect our ability to project military power. In 2007, Idaho National Laboratory conducted a demonstration using cyber tactics to destroy an electric generator[11] - the same type of generator

used on national power grids. In 2000, a disgruntled Australian employee used radio controlled Supervisory Control and Data Acquisition (SCADA) systems to discharge valves releasing raw sewage into water supplies 46 times over a two month period.[12] In the U.S., control of SCADA systems are available with an ordinary Internet connection and cellular telephones. In 2009, sensitive data was stolen from information systems supporting the Joint Strike Fighter program.[13] If we were to apply acts of cyber hostility to a specific location, at a specific time and in conjunction with a specific adversary's operational objective, we could see the impact on military planning, employment, and operations. For example, if these incidents took place on the island of Oahu in Hawaii immediately preceding a Pacific regional act of aggression by an adversary, military operations could be seriously impacted. Oahu is home to the U.S. Pacific Command and all service component headquarters and numerous operational forces including the 25th Infantry Division and the Pacific Air and Space Operations Center to name a few. According to the 2009 Quadrennial Defense Review,[14] the DOD currently operates more than 15,000 different computer networks across 4,000 military installations around the world. On any given day, there are as many as seven million DOD computers and telecommunications tools in use in 88 countries using thousands of warfighting and support applications. The number of potential vulnerabilities, therefore, is staggering. Moreover, the speed of cyber attacks and the anonymity of cyberspace greatly favor the offense. This advantage is growing as hacker tools become cheaper and easier to employ by adversaries whose skills are growing in sophistication.

RECOMMENDATION

1. The DOD should consider establishing a CCA within the joint command and control function to ensure the unique space, time, and force characteristics of cyber capabilities combined with inherent capabilities within our interconnected operational environment do not become a decisive advantage for our adversaries. Existing joint functions serve operational planners and war fighting units well. In fact, offensive and defensive computer network operations logically fit into joint fires and protection functions respectively. What it lacks is a centralized coordinating authority similar to the Space Coordinating Authority. Given the global characteristics of cyber capabilities, it's unlikely that cyber forces from the different services and agencies would deploy to the geographic theater of operations. The CCA is necessary to coordinate joint cyber operations and integrate cyber capabilities from the different components and supporting agencies. The CCA and supporting staff would facilitate coordination, planning, execution and assessment of joint cyber operations for the combatant commander to achieve theater specific objectives. Because of the global strategic nature of the cyber domain the CCA would also be responsible for serving as a planning liaison and deconflicting cyber operations in other geographic commands that could affect theater or operational objectives.

2. This structure would apply to all Combatant Commanders and would enable deliberate planning and operations in defending the U.S. against a sophisticated cyber attack. As mentioned earlier, a structure already exists in the command and control joint function in the Space Coordinating Authority. Where it becomes complex is when an enemy (state or non-state sponsored) targets cyber systems and networks that are intertwined with civilian infrastructure on American soil. Under the Homeland Security Act of 2002, the DHS is responsible for protection of critical infrastructure and cyber defense within the U.S. Inside the DOD, U.S. Northern Command (NORTHCOM) owns the mission to anticipate and conduct homeland defense and civil support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests. When it was created in 2002 NORTHCOM consolidated

under a single unified command existing missions that were previously executed by other DOD organizations. This provides unity of command, which is critical to mission accomplishment. The CCA under the NORTHCOM commander would be responsible for planning and executing consolidated cyber defense operations in times of crisis such as those highlighted in the earlier scenario. NORTHCOM could also provide the command and control of cyber forces to defend privately owned and operated critical infrastructure whether in support of DHS or as a supported command.

COUNTERARGUMENT

1. The first of two counterarguments pertains to legal authorities between the military, federal and state governments, and the private industries that own and operate critical infrastructure and key resources, but there is already precedence in dealing with these issues that have shown positive effect. First, the establishment of U.S. Cyber Command as a sub-unified command under U.S. Strategic Command has bridged civilian and military authorities under Title 10 and Title 50 of the United States Code. The commander, U.S. Cyber Command also retained the position as the Director of the National Security Agency and can leverage resources and operations in both components to leverage both Title 50 intelligence collection and Title 10 cyber defense operations. The second example is the National Counterproliferation Center (NCPC) under the Office of the Director of National Intelligence. This center brings together components from 16 different government departments and agencies. The NCPC does not duplicate the functions already performed by the individual Intelligence Community agencies. Instead, NCPC provides overarching leadership to integrate the efforts of the Intelligence Community to meet policymakers' counterproliferation priorities. This includes all issues, ranging from analysis and collection to interdiction. In both examples we demonstrate it is possible to operate within existing legal authorities and accomplish operational objectives.

2. The second counterargument is the establishment of a CCA doesn't give the Geographic Combatant Commander operational control of cyber forces in his theater and these forces must be assigned to a Joint Force Commander to accomplish operational objectives. Furthermore, the CCA creates an unnecessary layer of coordination that could detract from timely accomplishment of cyber objectives within the operational theater. This is a legitimate counterargument, but one that is outweighed by the unique operational factors defining cyber capabilities. The cyber fight is not limited to specific geographic boundaries and as demonstrated in this paper attacks in different theaters of operation can have distinct effects on a regional commander's ability to project military force locally.

CONCLUSION

In conclusion, the compelling argument for establishing a CCA is it brings coordinated defense of an interconnected operational environment while synchronizing and consolidating U.S. cyber power against operational and strategic objectives. Additionally, it recognizes cyber capabilities for what they are – another tool in the commander's box. It doesn't change the nature of war or how we conduct it, but like land, sea, air, and space power, applying it in the wrong way could change the outcome of operations.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations*. Change 1 (13 Febuary 2008) Joint Publication (JP) 3-0. (Washington, DC: CJCS, 17 September 2006). II-22-24.
2. Milan Vego. *Joint Operational Warfare: Theory & Practice*. (Newport, RI: Naval War Press, 2007), III-29.
3. Ibid.
4. Ibid. XIII-30.
5. White House. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. (Washington, DC: The White House, 2009). 1.
6. The term "Global Information Grid" was formally defined in a memo from the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence dated 22 September 1999, as "The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."
7. U.S. Department of Homeland Security. Homeland Security Presidential Directive 7. December 17, 2003(amended March 2008). http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1
8. U.S. Department of Homeland Security. National Infrastructure Protection Plan. 2009. 12.
9. Ibid. 3.
10. U.S. Congress. Senate. The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid: Hearings before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology. 110th Cong., 1st sess., 2007. 10.
11. Ibid. 53.
12. Ibid. 54.
13. Siobhan Gorman, August Cole and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project," Wall Street Journal. April 21, 2009, Technology Section. http://online.wsj.com/article/SB124027491029837401.html
14. U.S. Department of Defense. Quadrennial Defense Review Report, (Washington, DC: Government Printing Office, 2010). 37.

BIBLIOGRAPHY

Air Force Space Command. "The United States Air Force Blueprint for Cyberspace." Peterson AFB: Air Force Space Command, November 2, 2009.

Behar, Richard. "World Bank Under Cyber Siege in Unprecedented Crisis." FoxNews.com, October 10, 2008. http://www.foxnews.com/printer_friendly_story /0,3566,435681,00.html

Brenner, Susan W. Cyberthreats: The Emerging Fault Lines of the Nation State. New York: Oxford University Press, 2009.

Department of Defense. Military Power of the People's Republic of China 200 9. Available [Online]: http://www.defenselink.mil/pubs/pdfs/China_Military_Power_Report_2009.pdf

Department of Homeland Security. National Infrastructure Protection Plan 2009 Available [Online]: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Gorman, Siobhan, August Cole and Yochi Dreazen. “Computer Spies Breach Fighter-Jet Project.” Wall Street Journal. April 21, 2009. Technology Section Available [online]: http://online.wsj.com/article/SB124027491029837401.html

Harris, Shane. “The Cyberwar Plan.” *National Journal Magazine*. November 14, 2009. Available [online]: http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php

Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz, Cyberpower and National Security. Washington, D.C.: Potomac Books, 2009.

Libicki, Martin C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge, England: Cambridge University Press, 2006.

—. Cyberdeterrence and cyberwar. Santa Monica: RAND Corporation, 2009.

—. Who Runs What in the Global Information Grid. RAND Corporation, 2000.

Petruno, Tom. “Tribune, Google Trade Blame in United Airlines Stock Fiasco.” Los Angeles Times, September 9, 2008. Business Section.

“The Theft That Nobody Saw.” The Economist, Vol. 351, Iss. 8121 (May 1999): 23.

The White House. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications infrastructure. Washington, DC: The White House, 2009.

U.S. Congress. Senate. Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure: Hearings before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology. 110th Cong., 1st sess., 2007.

—. The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid: Hearings before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology. 110th Cong., 1st sess., 2007.

U.S. Senate. Congress. Federal Information Security Management Act of 2002. Washington D.C. 2002.

U.S. Department of Defense. Quadrennial Defense Review Report. Washington D.C. 2010. U.S. Office of the Chairman of the Joint Chiefs of Staff. Dictionary of Military and Associated Terms. (as amended through 31 October 2009). Joint Publication (JP) 1-02. Washington, DC: CJCS, 12 April 2001.

—. Joint Operations. Change 1 (13 Febuary 2008) Joint Publication (JP) 3-0. Washington, DC: CJCS, 17 September 2006.

—. Information Operations. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

—. Joint Operation Planning. Joint Publication (JP) 5-0. Washington, DC: CJCS, 26 December 2006.

U.S. Office of the Director of National Intelligence. National Intelligence Strategy Aug 2009

Available [Online]: http://www.dni.gov/reports/2009_NIS.pdf

Vego, Milan. Joint Operational Warfare Theory and Practice. 2007. Reprint, Newport: U.S. Navy War College, 2009.

The Cyberspace Domain: Recommendations to Change Mindsets and Air Force Culture
Major Joy M. Kaczor, U.S. Air Force (SAF/A6OT)

ABSTRACT

On 5 December 2005, the Air Force expanded its mission…'to fly and fight in Air, Space, and Cyberspace.[1] In 2008, cyberspace was officially introduced as the fifth military domain, alongside air, sea, land, and space.[2] The White House recently described cyberspace as an integrated domain critical to national security during peacetime and wartime.[3] This new domain is rapidly evolving as are cyberspace operations and missions enabled by cyberspace. To meet these changes, the cyber community is still restructuring and transforming how it organizes, trains, and equips for the cyberspace mission. History indicates that establishment of new domains drive cultural changes to adapt to and integrate new missions.[4] Thus, the Air Force culture must evolve in order to integrate cyberspace operations into the full spectrum of operations; however, the mindset within the cyber community must transform first. Cyber operators need to have an operational perspective and be able to develop strategy to support full spectrum operations. Furthermore, the change in mindset extends beyond the cyber community and into intelligence and other operational communities. Therefore, the cyber community must reach out to officers and NCOs through training and education to provide a common understanding of cyberspace operations in order to modify their mindset and facilitate a cultural change throughout the Air Force.

DESCRIPTION OF ISSUE

1. When the Air Force converted the communications and information force to cyber operations in 2010, the initial changes focused on Air Force Specialty Codes (AFSC) across the community, not mindsets.[5] The general mindset of the cyber community has been slow to transform to fully comprehend the requirements and scope of cyberspace operations. In the past, the introduction of a new domain forced a culture change in the Air Force. Thus, with the introduction of the cyberspace domain, the Air Force culture must evolve to truly embrace cyberspace operations and integrate it into the full spectrum of operations. In order for Air Force culture to change, the cyberspace community must first transform their mindset to facilitate the evolution in Air Force culture writ large. Cyber operators were converted to an operational career field (AFSC) without training specifically focused on operations and operational planning. In order to truly become part of the operational community, cyber operators need to understand and be able to plan and integrate cyberspace operations into full spectrum operations. To further the cultural change, the Air Force as a service needs to understand the role and importance of the integrated cyberspace domain and of cyberspace operations.

2. The Department of Defense (DOD) does not have a common cyber lexicon, which results in miscommunication and misuse of terms, specifically the use of cyberspace. To the cyber community's dismay, there are several definitions of cyberspace and cyberspace operations throughout government, military, academia, and industry. The original military definition, approved by the CJCS, in the National Military Strategy for Cyberspace Operations (NMS-CO) defined cyberspace as "a domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchange information via a networked information system and physical infrastructures."[6] In 2008, a memo from the Deputy Secretary of Defense, Gordon England, declared cyberspace as the fifth military domain and

defined it as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] This is now the official definition in Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, which the Air Force accepted in its guiding document on cyberspace, Air Force Directive Document (AFDD) 3-12 on Cyber Operations.[8] However, this definition varies significantly from the original definition provided by the NMS-CO, which included the electromagnetic spectrum. The official definition of cyberspace is broad and used to describe many issues. There is also debate on the current definition's exclusion of the electromagnetic spectrum. The confusion and resulting debates on the definition of cyberspace make the role of cyberspace unclear. The definition of cyberspace operations furthers obscures its meaning and how they can be integrated into full spectrum operations. JP 1-02 defines cyberspace operations as **"**the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid (GIG)."[9] This definition doesn't address operations to prevent adversary freedom of movement in the domain.

3. The ubiquitous nature of cyberspace and the ambiguous definitions and guidance have resulted in the slow change of mindsets. The cyber community is still restructuring and transforming how it organizes, trains, and equips to support cyberspace and enable cyberspace operations. In 2010, five years after the Air Force accepted cyber as a new domain; it transformed the communications and information force to cyberspace operations. The AFSCs of approximately 3,000 former 33S officers and 27,000 enlisted forces were switched to cyberspace specialties.[10] The current cyber corps have a diverse background of roles, experience, training, and education and thus lack a common understanding of cyberspace operations and how to integrate cyber into full spectrum operations. The current leadership in the cyber community matured as communications and information officers focused on technology, systems, and networks. Hence, the mindset of many is still network focused. Unfortunately, the cyber community will not have its first O-6 cyberspace operator who has fully matriculated through the new cyber training and education construct until 2025. However, due to the rapid evolution of cyberspace, the Air Force doesn't have the luxury of waiting until 2025 to transform the culture. Transformation must start within the cyber community and the conversion of AFSCs was a means to initiate the transformation across the Air Force. As Brigadier General Cotton, then director of cyberspace transformation and strategy at the Air Staff, said, "it's not just spray paint, it's a new mindset."[11]

4. The former communications and information community didn't have a strong requirement for intelligence nor a close relationship with the intelligence community. The evolution of cyberspace and dependence on intelligence for cyberspace operations forged a new relationship. However, the relationship between the cyber and intelligence communities and their interdependence are not fully understood, nor are intelligence requirements for supporting cyber operations. Most cyberspace operations are classified and many use tools or capabilities that are classified and require a "need to know." Additionally, the intelligence community has the authority and responsibility for conducting computer network exploitation (CNE). While computer network defense (CND) and computer network attack (CNA) are dependent on intelligence.[12] However, the majority of the cyber community doesn't have access to

intelligence products and the classification levels of cyberspace capabilities and operations prohibit many in the community from having a comprehensive understanding of cyberspace operations. This further complicates the cyber community's ability to define intelligence requirements for cyberspace operations.

5. The most recent, unclassified, guidance from the White House described cyberspace as an integrated domain that "traverses the physical domains of land, air, sea, and space."[13] Additionally, "the Air Force has concluded that the cyberspace domain underpins every aspect of warfighting simultaneously at all levels of operations and that cyber capabilities are being rapidly developed as well as globally dispersed."[14] Sheldon asserts that "cyberpower in the hands of a commander who is able to exercise all the imperatives of command will be a very powerful tool."[15] What Sheldon describes here is the need for commanders to focus on the mission and not the technology, and to structure their command to support the mission.[16] Consequently, the operations community needs to understand the role and importance of cyberspace as an integrated domain and how cyberspace operations can be employed in full spectrum operations.

RECOMMENDATION

1. Convertino et al. propose five recommendations "to enable the Air Force to effectively 'fly and fight' in cyberspace."[17] The first two directly support the recommendation for clear definitions and guidance. First, "the Air Force needs a clearly articulated cyberspace operating concept, hardware and software tools, and a dedicated, trained Cyber Warfare Corps."[18] Second, "the Air Force should clearly define and distinguish the military operations and effects it expects to achieve with the signals, data, information, knowledge, and intelligence flowing through and resident in cyberspace."[19] The cyber domain is not specific to the Air Force, therefore, the Department of Defense needs to establish a clear definition, theory, and supporting doctrine for cyberspace for the services to follow. A clear, unambiguous definition will provide the foundation by which operations in and through cyberspace can be defined. Kuehl proposes a new definition, "an operational domain whose distinctive and unique character is framed by the use of electronics, and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures."[20]

2. Cyber operators need to transform their mindset to comprehend their role in the broader operational community. The focus on support needs to transform to that of mission assurance and enabling operations. Cyber operators need to understand and be able to plan and integrate cyberspace operations into full spectrum operations. It is imperative that mid-level cyber operators have knowledge and experience in operational planning to be able to plan operations to create effects in and through cyberspace to achieve mission objectives. Since strategy drives operations, cyber operators also need to understand how to develop strategy that will guide future cyber operations. The development of Cyber 200 and 300 courses for junior and mid-level cyber operators (officers and enlisted) at the Air Force Institute of Technology (AFIT) is a critical step to provide this foundational knowledge. All cyber operators attend Cyber 200 or 300, which provides a common baseline understanding of cyberspace operations, including presentation of classified capabilities.[21] Additionally, more cyber operators need to attend the School of Advanced Air and Space Studies (SAAS) to learn how to develop strategy. Likewise, more cyber operators need to gain operational experience through working in A3 and

J3 staffs. Furthermore, the new interdependence of cyberspace operations and intelligence requires that more intelligence officers and NCOs attend Cyber 200 and Cyber 300 courses and, likewise, cyber officers and NCOs need to attend intelligence courses.

3. Providing a common foundation across the force will build a more cohesive air, space, and cyber force for the future.[22] Smith's research investigated the Air Force culture and cohesion after the establishment of the space domain and identified three processes necessary for organizational transformation to achieve force cohesion. First, the Air Force concept of its task environment must be carefully aligned "with the perception of the environment held by general, political elements."[23] Second, Air Force strategy and structure must be aligned "to achieve the critical operational tasks, roles, missions, and functions at the heart of the vision."[24] Last, "the changed culture, realigned and reinforced elites, and revised priorities must be socialized across the organization."[25] To do this, Smith recommended beginning with PME, joint education, and "cradle to grave career progression."[26] Thus, the Air Force needs to integrate cyberspace doctrine into all levels of Air Force PME for officers and NCOs and incorporate it throughout the curriculum, not just as a single lesson. Similarly, a cyberspace operations primer course needs to be developed for senior officers, since cultural change needs to begin at the top. In order to do this, the Air Force first needs a cyber doctrine center that is incorporated into the Curtis E. LeMay Center for Doctrine Development and Education and in cooperation with the Center for Cyberspace Research (CCR) at AFIT. The cyber doctrine center should drive the integration of cyberspace operations with air and space operations, while providing the latest guidance to CCR for inclusion into Cyber 200 and 300 course curriculums. Moreover, non-cyber operators need to understand the role and importance of the integrated cyberspace domain and of cyberspace operations. Hence, integrating cyberspace doctrine into PME will provide a common foundation, enabling cyber integration into full spectrum operations and improving force cohesiveness.

COUNTERARGUMENT

1. The current budget constrained environment has resulted in limited resources, manning, and funding. This makes it difficult to expand training opportunities. The proposed recommendations require significant investment in resources, people, and time to establish an Air Force Cyber Doctrine Center, create the necessary doctrine, and develop courses for PME. It also requires an investment of people and time to attend training and education courses to establish a foundational understanding across the Air Force and to expand knowledge within the cyber community.

2. Additionally, air and space operators may contend that they don't have the time for additional training and education. They may also argue that they are not responsible for the cyberspace domain. Surveys from the initial Air and Space Basic Course in the late 1990s indicated that "Air Force officer corps recognizes that its members display careerist attitudes and identify primarily with their technical specialties."[27] Consequently, Smith contends that the "absence of a shared vision or sense of mission in the Air Force" is a result of officers turning to their own occupational specialty.[28]

CONCLUSION

The U.S. military is still learning how to navigate in the integrated cyber domain. Unfortunately, history has proven that change in organizational culture is slow. "Military culture is the linchpin that helps determine the ability to transform because it influences how innovation and change are dealt with."[29] Thus, the military, and specifically the Air Force, culture must change to embrace cyberspace operations in order to effectively fight and win in cyberspace. General Norton Schwartz, Chief of Staff of the Air Force recognized that a cultural change is needed in the Air Force, stating that "cyber operations reinforce and enable everything we do -from administrative functions to combat operations and we must treat our computers and networks similarly to our aircraft, satellites, and missiles."[30] Smith asserts that "true organizational change requires a cultural transformation,—not simply accommodation and incremental modification but changed organizational output in terms of structure, professional incentives, and changed professional behaviors."[31] He describes it as an active, internal, top-down process that must "begin with the clear definition of a single unifying mission."[32] The Chief of Staff of the Air Force recently redefined "air power" to include air, space, and cyberspace. The clarification and unification of the Air Force mission will hopefully help to guide the cultural change.

Transformation must begin within the cyber community. Cyber operators need to have a common understanding of the domain, their roles and responsibilities, and operations in and through the domain. The Air Force Roadmap for the Development of Cyberspace Professionals outlines the training and education requirements as well as the core competencies for the cyber force. The Roadmap resulted in the development of Cyber 200 for 6-8 year cyber professionals, and Cyber 300 for 8-15 year cyber professionals.[33] The new Cyber 200 and 300 courses provide this foundation for the community. The cyber community must also understand how cyberspace integrates into full spectrum operations in order to address mission assurance requirements and operational impact concerns. Similarly, those outside the cyber community need to gain an appreciation for cyberspace beyond information technology. Broadening PME to better integrate cyberspace operations throughout the curriculums will provide the entire force with a common understanding and appreciation. This will ultimately improve force cohesiveness and the Air Force's ability to effectively fly, fight, and win in air, space, and cyberspace.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Converntino, et al. "Flying and Fighting in Cyberspace," p.iii.
2. Deputy Secretary of Defense Memo, 2008.
3. White House Guidance Regarding the Use of "Domain," p.2.
4. Smith, "Air Force Culture and Cohesion," p.41.
5. Brig Gen Cotton, "Cyber Workforce Transformation Update."
6. NMS-CO.
7. Deputy Secretary of Defense Memo, 2008.
8. JP 1-02, p. 86 and AFDD 3-12, p. 1.
9. JP 1-02, p. 86.

10. Rolfsen, "3,000 Officers Switch to Cyberspace Specialty."
11. Gen Cotton quote to Air Force News article.
12. Mahoney, "Reflections on a Strategy for Computer Network Operations," p. 158-159.
13. White House Guidance Regarding the Use of "Domain," p.2.
14. Converntino, et al. "Flying and Fighting in Cyberspace," p.3.
15. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," p.106
16. Ibid.
17. Ibid., p. iv.
18. Ibid.
19. Ibid.
20. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem."
21. Brig Gen Cotton, "Cyber Workforce Transformation Update."
22. Smith, "Air Force Culture and Cohesion," p.49.
23. Ibid.
24. Ibid.
25. Ibid.
26. Ibid., p.50.
27. Ibid., p.46.
28. Ibid., p.47.
29. Siegl, "Military Culture and Transformation," p.103.
30. Gen Schwartz, Message to Airmen.
31. Smith, "Air Force Culture and Cohesion," p. 42.
32. Ibid., p. 48.
33. The Air Force Roadmap for the Development of Cyberspace Professionals, p. 25.

BIBLIOGRAPHY

Air Staff, AF/A3O (2010). The Air Force Roadmap for the Development of Cyberspace Professionals.

Air Force Directive Document 3-12 (2010). Cyberspace Operations. Retrieved from http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf

Converntino, Sebastian, DeMattei, Lou Anne, and Knierim, Tammy. "Flying and Fighting in Cyberspace," Air War College Maxwell Paper No. 40. Maxwell AFB, AL: Air University Press. Retrieved from http://www.au.af.mil/au/awc/awcgate/maxwell/mp40.pdf

Cotton, David, Brig Gen, SAF/A6O (2010). "Cyber Workforce Transformation Update." Retrieved from http://www.safxc.af.mil/shared/media/document/AFD-100621-010.pdf

England, Gordan (2008). "The Definition of Cyberspace." Memo to the Military Departments. Fahrenkrug, David, T. (2007). "Cyberspace Defined." The Wright Stuff. Retrieved from http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm

Joint Publication (JP) 1-02 (2010). Department of Defense Dictionary of Military and Associated Terms. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Kuehl, Dan (2009). "From Cyberspace to Cyberpower: Defining the Problem." Kramer, Franklin, Starr, Stuart, & Wentz, Larry (Eds.), Cyberpower and National Security. Washington, D.C.: National Defense University.

Mahoney, John, R. (2011). "Reflections on a Strategy for Computer Network Operations." Jeffrey l. Caton, John H. Greenmyer, Jeffrey L. Groh, and William O. Waddell, (Eds.), Information as Power: An Anthology of Selected United States Army War College Student Papers, vol 5 (pp. 145-161).

Rolfsen, Bruce (2010). "3,000 Officers Switch to Cyberspace Specialty." Air Force News. Retrieved from http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/

Schwartz, Norton (2009). Message to Airmen.

Sheldon, John (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. Strategic Studies Quarterly (pp. 95-112).

Siegl, Michael (2008). Military Culture and Transformation. Joint Forces Quarterly, 49 (pp. 103-106).

Smith, James (1998). Air Force Culture and Cohesion. Air Power Journal (p. 40-53). Retrieved from http://www.airpower.au.af.mil/airchronicles/apj/apj98/fal98/smith.pdf

White House (2011). Guidance Regarding the Use of "Domain."

The Overstated Uniqueness of Cyberspace Operations

Major Jeffery A. Naylor, U.S. Air Force (AFIT)

ABSTRACT

The concept of Cyberspace operations as unique exists because it is the latest major evolution of warfare. Like most evolutions of warfare, in their time, there is a belief that Cyberspace operations transcends or at least circumvents the way we currently wage war. History is littered with examples of the battlespace changing because a new technology, weapon, or a domain emerges, but eventually warfighters adapt and the principles of warfare remain unchanged. However, the process of adapting to a changing battlespace is not aided when military thinking believe they do not need to change or that the new technology, weapon, or domain cannot be adapted. To this extent, the culture of uniqueness among cyber personnel is preventing cyber operations from fully maturing.

DESCRIPTION OF ISSUE

According to Maj Gen Vautrinot, (former 24 Air Force Commander), "When we talk about cyber, we are talking about “the mission,” or more precisely mission focus and mission accomplishment. My mission focus, just like in any other domain—whether it is ground, sea, air or space—the same is true for cyber: we are responding to orders and guidance that support this nation in its responsibilities and national security efforts around the globe." (Davis, 2012).

Cyberspace is certainly the new domain of warfare. However, not a single military member (i.e. the junior operators to the most senior leaders) is quite sure how Cyber fits into the way we fight. Senior leaders from Gen. Shelton to Gen. Alexander seem convinced that the way to move forward in Cyberspace is through “operationalization and normalization,” but operators continue to say that uniqueness is one of the defining characteristics to Cyberpower (Carr, 2010). Certainly, Cyber is an emerging domain whose parameters are still being defined, and that makes it different from the more established domains (Kramer, 2006). The word “unique” is fairly specific according to Merriam-Webster’s Dictionary (2012):

a. being the only one – sole
b. being without a like or equal – unequaled

Is Cyberspace the only sole domain of its kind? Is it unequalled? More importantly, if Cyber is “unique” then how can it be operationalized, let alone normalized? Ironically, Cyberspace is not the first evolution of warfare that has been thought of as unique. In fact, Cyber is certainly not unique compared to previous changes in warfare, and should stop being referred to and treated as unique if operationalization and normalization is the goal. Perhaps, there are lessons that previous changes in warfare can offer.

Technology has always driven warfare. From the wheel of a chariot to a Nuclear Intercontinental Ballistic Missile, evolutions in warfare have been driven by technological advancement. Technological advancement in antiquity did not occur because the military paid a company to develop a capability. Instead society developed something that would improve daily life. In that way Cyberspace technology can more closely resemble developments of the pre-military industrial complex technologies vice contributions that lead to the development of missiles, tanks, and airplanes. Bronze working and metallurgy for instance was used to create

tools and buildings. It took the Greeks of Sparta to prove that bronze working had a military application. For years Greek city-states had warred amongst themselves, but it was not until the battle of Thermopylae in 480 B.C. that the bronze clad Greek phalanx proved itself superior against the greatest military force ever assembled to that point in the history of war. No two historians agree on the size of the military forces at Thermopylae, but most estimates agree that the Greeks were outnumbered 50:1 and that the Persians suffered losses close to 10:1 (Keegan, 1993). The Greek phalanx would dominate warfare for the next thousand plus years. The phalanx moment in history is marked by two discernible features. First, the Greeks had practiced the phalanx tactics for hundreds of years. During that time they refined every aspect of phalanx warfare from the strategic to the operational. Second, the Spartans were the most professional military city-state in Greece. They knew the best terrain, were technically proficient, and their leaders understood the strengths and weaknesses of the phalanx. Thermopylae may have been the signature moment that defined warfare's first major evolution, but it was hundreds of years of refinement in the making. The technological challenges that define cyber require a professionalism and technical refinement that exceeds our current commitment.

The dawn of the middle age saw the rise of cavalry as the dominant arm of military operations. For a thousand years cavalry suffered in the shadow of a well employed phalanx. Cavalry tactics had been well established since Alexander the Great, but horses were unwieldy and precise phalanx movement easily relegated enemy cavalry to being a supporting arm of military operations. Cavalry does not have a moment like Thermopylae, but it does have some technological advancement that precipitated its rise. First, the bit in a horse's mouth allowed the cavalry to make tighter turns, which resulted in cavalry finally being able to out flank the infantry. Second, lighter stronger mail and plating meant that cavalry was survivable in a head-on charge against the infantry. These factors created the rise of heavy cavalry and it would dominate warfare for almost 700 years (Keegan, 1993). There was only one problem with heavy cavalry, it was expensive. Maintaining a horse, buying the armor, and even having the time for dressage meant that only upper-class noblemen could afford to be heavy cavalry. In many ways, the financial burdens of warfare in the middle-ages actually change the face of society as much as warfare. The feudal system was predicated on maintaining heavy cavalry. Cavalry's ability to be both precise and overwhelming was intimidating and led to the de-evolution of warfare. Militaries retreat to their well-built strongholds. Siege warfare was expensive and the outcome uncertain (Keegan, 1993). The similarities in Cyberspace are just as evident. Cyber power can be precise and overwhelming, and so, there is a tendency to be defensive in cyberspace.

However, the better lesson for Cyberspace may lay in the death of cavalry and the feudal system. The Battle of Agincourt is nearly as impressive a moment in military history as Thermopylae. The battle pitted 8,000 Englishmen (including 7,000 peasant longbow-men and zero cavalry) versus 50,000 Frenchmen with over 1,000 heavy cavalry (Keegan, 1978). The results were astonishing. The Welsh Longbow required no aiming, but instead was fired high into the air in a barrage fashion. The velocity the arrow achieved was able to pierce the heaviest of armor. The operator of a longbow only needed to be strong enough to pull the string back. This meant virtually anyone could be a longbow-man. This innovation once again gave rise to the concept of the citizen soldier. The rag-tag outnumbered, ill-trained English eviscerated the French killing nearly 10,000 and losing only 450 (Keegan, 1978). While muskets and canons would dominate

warfare within the next hundred years, it was the longbow that changed the face of war. Melee infantry and horse born cavalry would never again be the dominate forces of the battlefield. It is this evolution of past warfare that holds the most promise for cyberspace. On some level cyber has the ability to negate or destroy the effects of a 2 billion dollar plane. Cyber has the capacity to shut down a nation's nuclear capability. Current Cyber capabilities, similar to the emergence of the longbow, have the ability to render more expensive and specialized weapons irrelevant. Agincourt caused warfare to evolve much more quickly than it had in the past. The longbow was a force and a force multiplier. Siege warfare was cheaper, because an army of longbows could be fed more cheaply, and more easily reach the top of enemy defenses. Cyber seems to be playing a similar but even more profound roll. Cyber power does not require its operator to leave his cubicle and given enough time can pierce virtually any enemy defense, remotely.

The Battle of Agincourt had another technological advancement present, one of the first western cannons. Although, the Chinese have been using gunpowder for hundreds of years, the western world had not adopted it yet. The English cannons at Agincourt were still primitive, but they were the start of the artillery age of warfare. In the brief span of 300 years, the western world went through a reformation, renaissance, multiple revolutions, and a great deal of war. European countries began to build elaborate, vast, and bunkered forts to defend against the explosive power of canons and muskets. Canons made great siege weapons, but they were unpredictable on a pitched battlefield (Keegan, 1978). Like cavalry it is hard to pinpoint exactly when artillery became the dominant arm of military operations, but the greatest pioneer of artillery was most certainly Napoleon Bonaparte. Fratricide was a very real concern, but Bonaparte did two things to successfully mitigate this threat. First, his troops marched to battle in column formation instead of in a line (like they had since ancient Greece). If artillery was imprecise, this would mitigate and reduce the number of French casualties. Second, Napoleon demanded his artillery fire be clustered and more precise through the use of battery fire and physics to plan out artillery strikes before the battle. Napoleon was willing to attack the frontlines of his enemy instead of shooting at rear echelons (Keegan, 1978). The interesting thing is that neither of these innovations was new. Napoleon simply adapted concepts that already existed. Column movements have always been the preferred method of marching over long distances, and closely planned battery fire through physics was used to siege forts in the early 1600's. Similarly, Cyber operations are constantly being used outside of the box. Social engineering, spearfishing, denial of service, viruses, and Trojans are not new concepts. The art of cyber warfare lies in "how it is applied." Also, Napoleon required excellent predictive planning of his adversary. Napoleon failed to do this twice, strategically against Russia and then tactically at Waterloo, and therefore suffered dire results. Cyber struggles with the same planning requirements, and while the consequences are dire, they are hardly unique.

Many great military and political strategists come out of this time period, most notably Clausewitz. His theories on war are a mainstay in military education. Yet, there is one significant part of this era of war that he ignores, but it was a defining characteristic of the time and it is a defining characteristic of Cyber warfare. Clausewitz does not examine the asymmetric aspects of war even though they certainly existed. Mercenaries were frequently used to raid, sack, burn, and often pillage European towns. The proper military professionals like Clausewitz tend to ignore that men like Napoleon preemptively used Hussars, Cossacks, and other mercenaries to shape the battlespace (Keegan, 1993). Clausewitz also completely ignores the

American Revolution. Truthfully, the professional ethical military that artillery gave rise to, was never completely real. There is, perhaps, a stark warning for the strategist of today implementing strategy into the cyber domain. Europe failed to understand that Napoleon viewed the whole of Europe as a battlefield. This same concept is how the North won the American Civil War. New battlespace are rarely well defined by laws of conflict. If your adversary, hypothetically China or Russia, believes there are no innocents in the new battlespace, then they have a strategic and operational advantage over you. More importantly, that is an advantage that technical and tactical proficiency will not overcome. The evolution of warfare could go on endlessly: the rise of naval power and shipping lanes, the railroad for logistics, aircraft, radar, and others. Each has fundamental and unique lessons that they share with cyber operations. However, the last evolution for this discussion will be the nuclear Intercontinental Ballistic Missile (ICBM). Most people are familiar with the concept of mutually assured destruction. Yet, it was a developed response over a number of years. Before the Cold War fully matured, many top officers were concerned that poor warning systems and untested procedures might result is not being able to retaliate. In other words, whoever launches first secures victory (Keegan, 1993). While this is the mark of an unrefined military discipline, it is also a strategic and operational fact. Until, the cyber battlespace is more predictable, planners need to account for gaining the operational initiative.

Cyber is certainly different than anything we have previously seen in warfare, but most evolutions in warfare are different when they are first introduced. There is no technology or domain that perfectly mirrors Cyberspace. Cyber operations require a highly specialized skill set, but it is no more specialized than a heavy cavalryman or a hoplite in a phalanx. There are significant technical considerations, but they are not as complex as astrophysics, aeronautical engineering, or nuclear science. While no two evolutions in war are completely the same, they all share similar characteristics. Perhaps, skipping parts of history weakens the argument that cyber is merely different and new, but the opposite is more likely true. The truth is that cyber's characteristics are not unique in a historical context. Cyber is at best unusual because it is perceived as entirely man-made, but it still resides in the electromagnetic spectrum (which is a natural physical environment). All constructs and weapons of war are manmade, and all domains have a physical realm. The notion that cyber is unique as a man-made domain is fatuous. Mankind has always sought to control the parameters of his battlespace. Just because man created a little more of the battlespace does not change the objective of shaping it.

RECOMMENDATION

So where does Cyber Operations go in light of historical context. First, stop referring to the uniqueness of cyber operations. The concept of cyber as unique is alleviating Information Technology (IT) personnel from developing a warrior ethos. If IT continues to believe they are unique and other operators just do not understand them, then they will never become the Cyber-Warriors and Cyber Leaders the military so desperately needs. Second, Cyber Operators need to start speaking in term of effects. A pilot does not tell you about the physics of maneuver, they tell you about the bomb they dropped or the Aircraft they killed. Cyber needs operators who are technically proficient, battlefield savvy, and speak operations like the Spartans, Knights of the middle-ages, and Napoleon's artillerymen. Lastly, focus on ways domains and technologies have integrated in the past. History is littered with examples that have some applicability. Just because an analogy with previous evolutions of warfare is not perfect does not mean it is devoid of merit. The more Cyber Operations is treated like other Operations, the more quickly the

process will move. Military leaders will not accept baffling technical answers from other operators…why should they have to from cyber operators? This needs to stop if we are going to operationalize and normalize cyberspace. Finally, potential adversaries must not be allowed to define the battlespace and/or seize the operational initiative. Cyber warfare is still largely ungoverned under the Law of Armed Conflict and International Law (Jabbour, 2010). If an adversary believes there are no cyber innocents, then the United States military act to protect the (intellectual) property of it citizens.

CONCLUSION

The concept of a uniqueness attribute in cyber operations is inhibiting our ability to adapt to the cyberspace environment. Instead of comparing cyber to current domains, technologies, and weapons of warfare it should be compared to previous evolutions of warfare. Finally, vigilance is required in a new domain. When laws are not established or easily ignored in a domain, history shows, someone will leverage unethical practices to gain a strategic advantage. If the United States is unwilling to retaliate swiftly and sternly, then the citizens we defend will ultimately pay the price.

REFERENCES

Carr, Jeffrey, and Lewis Shepherd. Inside Cyber Warfare. Sebastopol, Calif.: O'Reilly Media, Inc., 2010.

Davis, Auburn. "Maj Gen Vautrinot discusses the importance of cyber operations." Air Force Print News Online. Available from http://www.afspc.af.mil/news1/story_print.asp?id=123298320

Jabbour, Kamal. "Cyber Vision and Cyber Force Development." Air University. www.au.af.mil/au/ssq/2010/spring/jabbour.pdf

Keegan, John. A History of Warfare. New York: Alfred A. Knopf, 1993.

Keegan, John. The Face of Battle: A Study of Agincourt, Waterloo and the Somme. Harmondsworth, Middlesex: Penguin Books, 1978.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. Cyberpower and national security. Washington, D.C: Center for Technology and National Security Policy, 2009. Cartledge, Paul. Thermopylae: the battle that changed the world. Woodstock, NY: Overlook Press, 2006.

"Unique - Definition and More from the Free Merriam-Webster Dictionary." Dictionary and Thesaurus - Merriam-Webster Online. Available from http://www.merriam-webster.com/dictionary/unique

Tablet Computers will Enhance Military Operations
Major Thaddeus J. Janicki, U.S. Air Force (953 RSPTS)

ABSTRACT

This paper highlights the use of tablets on military computer networks. Tablets have gained popularity recently due to the release of Apple's iPad and several Android tablets. Tablets are an effective use of new information technology, and military leaders are starting to see a promising future by integrating tablets in daily operations. Consider operations such as a soldier on the front line with a tablet in hand controlling a camera on an Unmanned Aerial Vehicle (UAV) to getting a real-time assessment of the battlefield, or a pilot flipping through multiple flight pattern maps to devise a flight path for their next mission. As with any computer-like device, tablets have vulnerabilities that administrators will need to keep at bay. Vulnerabilities such as computer viruses or hackers could easily do more harm than good by negating any tactical advantage gained on the battlefield. New policies and procedures will need to be developed on the use of tablets to thwart vulnerabilities and security breaches. Tablets can easily provide numerous advantages throughout the military, but it is clear that there are significant disadvantages that need to be addressed before military leaders choose to deploy tablets on military networks.

DESCRIPTION OF ISSUE

1. The military currently uses an estimated 80,000 mobile devices for cyberspace activities.[1] A subset of that number, tablet computers, can aid the operator in mission completion. Military leaders are looking to hone in on this benefit to provide them to operators, "who require secure real-time information at their fingertips to execute their mission."[2] Air Force leaders are exploring ways to provide their pilots with digitized aerial maps and real-time Situational Awareness (SA) for first responders. The Army is looking for solutions to provide interoperability among various communications systems to provide SA and Close Air Support (CAS) to forward deployed militry.[3] One example of the usefulness of tablet computers was an exercise performed by the Army. "Soldiers were able to see everyone's position in the group, talk over networks, exchange data messages, and view live streaming video from an unmanned aerial vehicle (UAV). They also were able to collaborate on devices using a whiteboard software application: Pictures drawn on one smart phone or tablet were broadcast to other devices in the network, even in dense foliage."[4] Another app will allow soldiers to use their tablets as a digital map that can scan the horizon and use digital markers to display orientation and objective issues.[5] Still another allows expedited treatment of soldiers who are injured in combat by speeding requests for medical evacuation through exact locations of injured soldiers and menus that relay crucial personal information, such as health information and the type of injury.[6] These types of apps can not only bridge instant communication between military operations, but can achieve far more positive results on the field with more knowledge of the terrain and enemy movements. The geo-location feature of tablets can provide operators with situational awareness of the battlefield;[7] however, our adversaries would be able to utilize that same feature to locate every soldier if they were able to hack into our tactical networks.

2. An article in the *National Defense* magazine stated, "Pentagon officials have a bad case of commercial electronics envy: They see all the smartphones and tablets that civilians use and they want to put those same gadgets into the hands of their troops."[8] The problem is that the military cannot acquisition the equipment and write policies fast enough to roll out new emerging

technologies. Acquisition times must be reduced to meet the rapid pace of IT advancements and policies governing the use of tablets must be available before implementation takes place.[9] Part of the reason that there are such limited devices available is because the procedures in place to acquire these devices are almost the same procedures for purchasing a weapon system. The normal process takes 91 months[10] from planning to approval, and that just will not work for today's fast moving technology marketplace. As part of the 2010 national Defense Authorization Act, Congress acknowledged the problem and enacted a mandate for the Pentagon to speed up the IT system acquisition process.[11] Once in law, this measure should provide a more realistic timeframe for interested agencies to purchase and use mobile technology. A similar problem that civilian companies face, to which the military is not immune, is that they failed to have a clear strategy of the use of tablets.[12] Department of Defense (DOD) will need to provide policies and education for the end-users to follow. To follow the security regulations within the U.S. Department of Defense, all computers operating on DOD networks must comply with established security protocols. These requirements include support for Windows operating systems, 802.11 Wi-Fi wireless network compatibility, and data-at-rest (DAR) encryption functionality, all while ensuring compliance with DOD Instruction 8500.1 Information Assurance (IA) security requirements. To ensure DOD computers and their operating systems meet established security requirements, the Defense Information Systems Agency (DISA) developed the "Gold Disk." The Gold Disk is a tool designed to assist developers and system administrators in successfully testing and securing the Windows operating system, desktop applications, and Internet Information Services in accordance with applicable IA standards. These IA standards are identified in the Gold Standard (Gold Policy), as well as DISA Security Technical Implementation Guides (STIGs). The Gold Disk standards set forth for desktop and laptop computers do not completely apply when utilizing handheld computers. Other actions, like software vulnerability scans, can cause confusion as well. Portable devices will not always be powered on, and may not be connected to the network at all times. These differences can raise questions when going through the IA certification and accreditation approval process for mobile devices. Without the existence or enforcement of policies for tablet use, users may take it upon themselves to add tablets to networks without authorization.[13]

3. By far, the most important downfall of tablets for the military is their lack of security. With attacks on mobile devices and networks on the rise, DOD cannot afford to ignore the need for tighter security, before they decide to allow these devices on military networks. A recent hacker convention in Europe demonstrated the ease with which attackers targeting mobile devices could quickly compromise systems. One attendee installed malware code and used an antenna array that acted as a cell tower, allowing him to take over control of all the mobile devices in the vicinity.[14] A Microsoft demonstration also hijacked the mobile phones in the building.[15] A survey conducted by Symantec Corporation in 2012 found that despite several security risks associated with mobile technology, most organizations are shifting toward deploying mobile technology. Their survey, also, found that mobile devices were categorized as a top-three IT risk by most of the IT decision makers.[16] In recent months, attacks on mobile devices and networks have been on the rise, both in numbers and sophistication.[17] Recently, the Air Force canceled plans to purchase 3,000 Apple iPad2s for unannounced reasons, but it is suspected to be related to the discovery of the Russian-developed app that was planned to be used to read sensitive flight charts and aircraft technical data.[18] In addition, a large threat to mobile computing devices comes from personnel losing their mobile devices.[19]

RECOMMENDATION

1. In the commercial sector, most customers demand quality in terms of speed, low cost, and long battery life. The military also desires these functions, but the tablets that the military dreams of using, first and foremost, must fulfill the requirements of SWP-C—size, weight, power, and cost.[20] "Typically [the military looks] for a small lightweight, handheld device with a touchscreen display, designed to include sufficient environmental sealing to withstand the extreme environments found in a military application…a tablet that is capable of being dropped in a puddle, exposed to sand and dust, withstand a high humidity environment, and operate with a gloved hand."[21] In close combat, the amount of equipment soldiers are carrying can often mean the difference between life and death.[22] At the same time, the tablet must be powerful enough to complete the necessary tasks in communication and information. The cost must be reasonable enough for the military to be able to purchase in bulk. The military has already spent $4.2 million in developing military applications and further studying smart phones.[23] Tablets and other mobile devices, however, are relatively inexpensive in today's market and cost around $400, in juxtaposition to $10,000 wireless receivers, making investments in this field particularly advantageous for the military.[24] In all, tablets are frequently used outdoors in all conditions, they must be extremely rugged, weather sealed, reliable, and easy to use since there may be no technical support in the vicinity. Tablets also need long-life batteries for all day operation in the field, and enable a simple battery swap when it is needed. They need to meet the security and software compatibility requirements developed for desktop and laptop models, be lighter, more rugged, more weather sealed for outdoor use, have extended battery life, be more ergonomic for portable use and must provide considerable additional functionality, such as support for automatic identification technologies (AIT) like bar code and RFID. They must also support peripheral devices such as Common Access Card (CAC) readers.

2. To tackle the cumbersome acquisition process, Gilligan Group Inc., a Virginia-based IT consulting firm, proposed a streamlined process. They were able to reduce the 91-month process to 18 months and reduced cost by 20 percent.[25] Weapon system acquisition projects tend to cost millions or billions of dollars, so saving 20 percent is a huge feat, but the benefit would be the reduction in time it takes to get these innovative devices into the hands of warfighters before they are obsolete. To accomplish the reduction in time, Gilligan Group Inc. suggests that the main requirements in the acquisition process be broken down to smaller projects that use templates to expedite development. Reduction of acquisition time will also require the need to reduce the time for policy implementation. DISA has been at the forefront of DOD's charge to get mandated policies that govern the use of tablets on military networks. DOD networks must comply with established security protocols. DISA released STIGs in late 2011 and early 2012 that provide security policy and configuration requirements for the use of Android and Apple mobile handheld devices.[26, 27] As of the date of these STIGs, there were no Apple iOS or Android-based tablets approved for use on any military network. These devices, however, could be used in a stand-alone mode of operation, as long as all wireless and Bluetooth, capabilities are disabled. Apple iOS and Android-based tablets will need first to gain FIPS 140-2 certification before they would be considered to join military networks. FIPS 140-2 certification mandates that these mobile devices use cryptographic modules to secure all data. Lower level policies and a clear strategy for the use of tablets will also need to be authored by the end-users' leadership. Tablets are not "one-size fits all" and will need careful evaluations to determine the needs of the intended users. Educating the warfighter about security vulnerabilities and protective measures

will also prove to be a challenge. The end-user will need to know how to protect the sensitive "operational" data on these devices, as well as use strong passwords or encryption devices to secure the data and to thwart unauthorized access.

3. DISA STIGs are attempting to reduce security vulnerabilities, but it is up to the manufacturer to eradicate them. For intrusion detection, the US Army's Communications Electronics Research, Development and Engineering Center (CERDEC) has recently created the Intrusion Detection System (IDS) as part of their Tactical Wireless Network Assurance (TWNA) Army Technology Objective.[28] The IDS detects if mobile nodes have been infiltrated and broadcasts network dangers. The IDS will eliminate any communications with the dangerous node. Another security measure is to address apps. According to DISA STIGs for both Apple iOS-based and Android-based tablets, the App Store and Android Market place, respectively, will not be authorized for use to download apps.[29, 30] This will prevent users from downloading apps that may have hidden code that allow hackers to create backdoors into military networks. DOD will need to have programmers and app designers to produce apps specifically created for the operators' tasks. Such apps should not be available for public use. Finally, the military can use zero client technology, a smartphone technology that operates without an operating system or software; the device operates only as a connector between the application running in a data center and the user.[31] This would prevent sensitive information from being stored on the individuals' mobile device; the data would now be stored on a secure server in the data center, much like a virtual private network (VPN). The data leaving the phone would be encrypted, so that it would be nearly impossible for anyone intercepting a transmission to interpret any useful information. The relocation of the data from a phone to a secure data center would enable the current security measures in place to be standardized, instead of being controlled by each issuing authority. This standardization would ensure the data protection, installed applications, and security is uniform across all users. This would not only reduce costs associated with monitoring and updating security policies, it would allow mobile devices to be monitored for compliance within the established security procedures.

COUNTERARGUMENT

1. Regardless of the many benefits that tablets can bring to the fight, they are still very vulnerable and add extra threats to the military networks. DOD simply cannot afford to have these vulnerabilities on their networks during a time when they need to maintain cyber dominance over our adversaries. Tablets are still an emerging technology and need to be improved before the military can seriously consider using them on their networks. The lack of security is the main reason why tablets have not made it into the hands of military members.

2. Another major setback to implementing mobile devices, tablets in particular, is the lack of wireless infrastructure in the area of operations around the world. DOD currently does not have the billions of taxpayer's dollars at their disposal to invest in the development and construction of wireless infrastructure and backbone needed by mobile devices. Not only is money an issue, but time is a factor as well. It will take years to develop and deploy the wireless infrastructures around the world.

3. Even though tablets cost less than some desktops and significantly less than most ruggedized laptops, they are still easier to lose and harder to repair. Tablet battery life cycles are significantly less than laptops and lack the ability to be replaced in the field. Unlike desktops

and laptops, tablets will need to be sent back to the manufacturer to have any major repair accomplished. Manufactures have been losing money for years on repair costs and they have adopted the lack of Field Replaceable Units (FRU) in tablets. Therefore, they are able to drive down the initial purchase prices, which are more appealing to budget restricted buyers, and still continue to earn revenue from tablets after the initial sale because they are the only ones who can service them.

4. The lack of trusted software applications substantially diminishes the capabilities of tablets and allure to military uses. iPad and Android tablets are known for their plethora of apps, but what customers don't realize is that the same apps that they are using can be, and in some cases, are designed for malicious intent. Some apps are sending personal and location information without the knowledge to the user. Therefore, DOD cannot allow their users to inadvertently install an app until it has been thoroughly tested. More than likely, DOD will never lift the ban to access the millions of apps that are available on the Apple's App Store and Android's Market Place. That poses the question "what are tablets really good for without access to the apps?" Again, it will take DOD years to test or develop their own apps that the military can trust to run on its networks.

5. With that all being said, are tablets really "cost effective" enough to mass deploy on military networks? Tablets are an emerging technology still in its infancy and DOD will need to seriously weigh the pros and cons of tablet use on military networks. DOD networks are simply not ready to mass deploy tablets and it will take time to mass deploy DOD wide.

CONCLUSION

1. Apple's iPad and the numerous Android-based tablets will clearly change the way military members do business on the battlefield. These tablets will provide a plethora of information at the warfighters' fingertips and allow them to make the most informed decision for any situation. Pentagon officials, however, are going to need to control their "commercial electronics envy" for the time being because tablet use on military networks is still in its infancy and demands time to work out the kinks. In order for these tablets to join military networks, they will need to offer tighter security features, clearer strategies of use, and policies to govern their use. DISA is at the forefront of developing and providing these necessities, but they will require help from the manufacturers to keep security in mind when developing new technologies for future use.

2. Emerging technologies in the wireless infrastructure realm are providing state-of-the-art capabilities. Such innovations are clearly being developed to answer the call of the military's demands of system interoperability and worldwide use.

3. With cyber-attacks on the rise on mobile networks and devices, military IT administrators will need to secure their networks in order to maintain our cyber dominance. Mitigating vulnerabilities are of the utmost importance, but educating the users about mobile devices uses can be just as imperative.

4. Finally, the question of whether tablets are "cost effective" to mass deploy on military networks will linger over military decision makers' heads for some time. Maybe military leaders should be asking themselves the question "Can we afford not to embrace tablet innovation throughout the military?" In the meantime, DOD will need to continue to use tablets in non-

operational environments until significant progress is made with securing these hacker-friendly devices.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Jim Tice, "Army Eyes Civilian Gadgets for Military Use," *Army Times,* 2008, 69(13). http://www.armytimes.com/news/2008/10/army_mobiledevices_101308w/
2. Harris Corp, "Harris Corporation Introduces Ruggedized Tablet for Defense and Public Safety Mission-Critical Communications," Business Wire (English), 2. Regional Business News, EBSCOhost.
3. Dusseau et al., "Network Centric Interoperability," Digital Avionics Systems Conference, 2003. DASC '03, p. 1.
4. S. Frink, "Army Demonstration of Commercial Cell Phone Technology on the Battlefield Relies on Raytheon Technology." *Military & Aerospace Electronics,* 2011, 22(12), 9.
5. Nathan Hodge, "Killer App: Army Tests Smartphones for Combat," *The Wall Street Journal.* 2011. http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html
6. Ibid.
7. Chris Carroll, "iPad, iPhones and Other Top Mobile Devices Still Banned from DOD Networks." *Stars and Stripes.* Last modified 05 Oct 2011. http://www.stripes.com/news/ipads- iphones-and-other-top-mobile-devices-still-banned-from-dod-networks-1.156997
8. Blake Johnson, "Security Is Priority as Feds Craft Plan for Mobile Devices." *Federal Times* 9, 2012. NewsBank online database (America's News).
9. Grace V. Jean, "Clamor for Mobile Devices May Help Speed IT Acquisition." *National Defense,* 2011, no. 693:37. Military & Government Collection, EBSCOhost.
10. Dusseau et al., Brock. Raytheon Technical Services Co., "Network Centric Interoperability." Digital Avionics Systems Conference, 2003. DASC '03.
11. Ibid.
12. Chris Carroll, "iPad, iPhones and Other Top Mobile Devices Still Banned from DOD Networks." *Stars and Stripes.* Last modified 05 Oct 2011. http://www.stripes.com/news/ipads- iphones-and-other-top-mobile-devices-still-banned-from-dod-networks-1.156997
13. Shara Tibken. "Here Come Tablets. Here Come Problems." *The Wall Street Journal,* April 2, 2012. http://online.wsj.com/article/SB10001424052970203986604577253162552946038.html?mod=WSJ_hp_mostpop_read#articleTabs%3Darticle
14. Grace Jean, "Clamor for Mobile Devices May Help Speed IT Acquisition." *National Defense,* 2011, no. 693:37. Military & Government Collection, EBSCOhost.
15. Ibid.
16. Symantec. "Mobile Security Incidents Costing Firms Nearly $500,000 a Year." (2012). http://www.v3.co.uk/v3-uk/news/2154670/mobile-security-incidents-costing-firms-nearly-usd500
17. 1105 Government Information Group, "Cyber Security." *Federal Computer Weekly.* www.FCW.com/SpecialReportCybersecurity

18. John Cox, "Air Force Abruptly Scraps iPad Plan for Special Ops." *Network World,* February 22, 2012. http://www.networkworld.com/news/2012/022212-air-force-ipad-256446.html?page=1
19. Symantec. "Mobile Security Incidents Costing Firms Nearly $500,000 a Year." (2012). http://www.v3.co.uk/v3-uk/news/2154670/mobile-security-incidents-costing-firms-nearly-usd500
20. Courtney E. Howard, "By Land, by Sea, by Air: Rugged Computers Are Everywhere." *Military & Aerospace,* 2010, 21(1), 32–46. http://www.militaryaerospace.com/articles/print/volume-21/issue-1/features/technology-focus/by-land-by-sea-by-air-rugged-computers-are-everywhere.html
21. John McHale, "Reliability, Small Size, and Fast Performance Drive Rugged Military Handheld Devices." *Military & Aerospace Electronics*, 2011, 22(9), 37–38. http://www.military aerospace.com/articles/print/volume-22/issue-9/product-intelligence/reliability-small-size-and- fast-performance-drive-rugged-military-handheld-devices.html
22. Matthew Cox. "Army to Battle-test Lighter, More Mobile Gear." *Army Times,* 2009, 69(36), 14–16. http://www.armytimes.com/news/2009/03/army_soldierload_032309w
23. Nathan Hodge, "Killer App: Army Tests Smartphones for Combat." *The Wall Street Journal.* 2011. http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html
24. Matt Hamblen, "iPads, Android Tablets and Smartphones Join the Military." *Computer World.* 2011. http://www.computerworld.com/s/article/9214624/iPads_Android_tablets_and_smartphones_join_the_military
25. Grace V. Jean, "Clamor for Mobile Devices May Help Speed IT Acquisition." *National Defense,* 2011, no. 693:37. Military & Government Collection, EBSCOhost.
26. Defense Information Security Agency (DISA) Security Technical Information Guide (STIG), *Apple iOS 4 Overview V1R1*, 20 Oct 2011, p. 1–40.
27. Defense Information Security Agency (DISA) Security Technical Information Guide (STIG), *Android 2.2 Dell V1R1 Overview,* 23 Nov 2011, p. 1–37.
28. Rita Boland, "Army Eliminates Enemies at Any Node." *SIGNAL Magazine,* April 2008. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1550&zon eid=231
29. Defense Information Security Agency (DISA) Security Technical Information Guide (STIG) *Apple iOS 4 Overview V1R1*, 20 Oct 2011, p. 8.
30. Defense Information Security Agency (DISA) Security Technical Information Guide (STIG) *Android 2.2 Dell V1R1 Overview*, 23 Nov 2011, p. 11.
31. Blake Johnson. "Security Is Priority as Feds Craft Plan for Mobile Devices." *Federal Times* 9, 2012. NewsBank online database (America's News).
32. F. Kramer et al, *Cyberpower and National Security.* (Washington, DC: Center for Technology and National Security Policy, 2009).

BIBLIOGRAPHY

1105 Government Information Group, First. "Cyber Security." *Federal Computer Weekly.* www.FCW.com/SpecialReportCybersecurity

Bacon, Lance M. (2011). "Tablets, Cellphones Give Soldiers 'Extra Edge.'" *Army Times.* http://www.armytimes.com/news/2011/11/army-tablets-cellphones-give-soldiers-extra-edge-111511/

Boland, Rita. "Army Eliminates Enemies at Any Node." *SIGNAL Magazine,* April 2008. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1550&zon eid=231

Carroll, Chris. "iPad, iPhones and Other Top Mobile Devices Still Banned from DOD Networks." *Stars and Stripes.* Last modified 05 Oct 2011. http://www.stripes.com/news/ipads- iphones-and-other-top-mobile-devices-still-banned-from-dod-networks-1.156997

Cox, John. "Air Force Abruptly Scraps iPad Plan for Special Ops." *Network World,* February 22, 2012. http://www.networkworld.com/news/2012/022212-air-force-ipad256446.html?page=1

Cox, Matthew. "Army to Battle-test Lighter, More Mobile Gear." *Army Times,* 2009, 69(36), 14–16. http://www.armytimes.com/news/2009/03/army_soldierload_032309w

Defense Information Security Agency (DISA) Security Technical Information Guide (STIG). *Apple iOS 4 Overview V1R1,* 20 Oct 2011.

Defense Information Security Agency (DISA) Security Technical Information Guide (STIG). *Android 2.2 Dell V1R1 Overview,* 23 Nov 2011.

Dusseau, Douglas, and Clinton Brock. Raytheon Technical Services Co., "Network Centric Interoperability." Digital Avionics Systems Conference, 2003. DASC '03. Erwin, Sandra I. "Ground Connections." *National Defense,* June 2008, 48–50.

Frink, S. "Army Demonstration of Commercial Cell Phone Technology on the Battlefield Relies on Raytheon Technology." *Military & Aerospace Electronics,* 2011, 22(12), 9.

Hamblen, Matt. "iPads, Android Tablets and Smartphones Join the Military." *Computer World.* 2011. http://www.computerworld.com/s/article/9214624/iPads_Android_tablets_and_smartphones_join_the_military

Harris, Corporation. 0002. "Harris Corporation Introduces Ruggedized Tablet for Defense and Public Safety Mission-Critical Communications." Business Wire (English), 2. Regional Business News, EBSCOhost.

Hodge, Nathan. "Killer App: Army Tests Smartphones for Combat." *The Wall Street Journal.* 2011. http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html

Howard, Courtney E. "By Land, by Sea, by Air: Rugged Computers Are Everywhere." *Military & Aerospace,* 2010, 21(1), 32–46. http://www.militaryaerospace.com/articles/print/volume-21/issue-1/features/technology-focus/by-land-by-sea-by-air-rugged-computers-are- everywhere.html

Jean, Grace V. "Clamor for Mobile Devices May Help Speed IT Acquisition." *National Defense,* 2011, no. 693:37. Military & Government Collection, EBSCOhost.

Johnson, Blake N. “Security Is Priority as Feds Craft Plan for Mobile Devices.” *Federal Times* 9, 2012. NewsBank online database (America’s News).

Kramer, F. D., S. H. Starr, and L. K. Wentz. *Cyberpower and National Security.* Washington, DC: Center for Technology and National Security Policy, 2009.

McHale, John. “Reliability, Small Size, and Fast Performance Drive Rugged Military Handheld Devices.” *Military & Aerospace Electronics,* 2011, 22(9), 37–38. http://www.militaryaerospace. com/articles/print/volume-22/issue-9/product-intelligence/reliability-small-size-and-fast- performance-drive-rugged-military-handheld-devices.html

Symantec. “Mobile Security Incidents Costing Firms Nearly $500,000 a Year.” (2012). http://www.v3.co.uk/v3-uk/news/2154670/mobile-security-incidents-costing-firms-nearly- usd500

Tibken, Shara. “Here Come Tablets. Here Come Problems.” *The Wall Street Journal,* April 2, 2012. http://online.wsj.com/article/SB10001424052970203986604577253162552946038.html?mod=WSJ_hp_mostpop_read#articleTabs%3Darticle

Tice, Jim. “Army Eyes Civilian Gadgets for Military Use.” *Army Times,* 2008, 69(13). http://www.armytimes.com/news/2008/10/army_mobiledevices_101308w/

PART VI: DETERRENCE AND RESILIENCE (OPERATIONAL)

Continuous Monitoring: Privacy vs. Protection
CW4 Elbert Peak, U.S. Army (AFIT)

ABSTRACT

Computer network monitoring is used for both offensive and defensive cyberspace operations. On the offensive side, computer attackers eavesdrop on network communications. On the defensive side, which is discussed in greater depth with respect to the privacy and protection of the network, cyberspace operators track the activity of attackers and insiders who misuse their networks. Many cyber warfare attacks can be averted by monitoring and controlling access to and use of information resources. Even if an offensive operation is not prevented, monitoring might detect it while it is in progress, allowing the possibility of aborting it before serious damage is done and enabling a timely response. One of the most controversial issues in recent years is how continuous monitoring threatens the privacy of users (Corcos, 2004). Today, several technologies and methods exist to better protect the network and personal data. It is proposed that certain monitoring techniques play an important role for the protection of networks. Before this goal can be achieved, however, many technical and ethical issues will have to be resolved.

DESCRIPTION OF ISSUE

1. An array of partial measures exists for countering the intruder and insider threat, but is limited in scope and capabilities. Many cyber warfare attacks can be averted by continuous monitoring and controlling access to and use of information resources. Even if an offensive operation is not prevented, monitoring might detect it while it is in progress, allowing the possibility of aborting it before any serious damage is done and enabling a timely response. This paper focuses on three defensive operations (or problem sets): access control, filtering, and intrusion and misuse detection.

The focus is on protecting government owned media, especially computers and networks, but also physical resources. Continuous monitoring applies to more than government owned resources, however. It covers open source media as well. Organizations can watch these media for propaganda that may be damaging to their interests. Continuous monitoring includes counterintelligence programs, particularly surveillance operations against insiders who seek classified or sensitive information of an organization. Defense poses unusual challenges: privacy rights. To date, the main focus of Information Technology (IT) security products has been on providing solutions to detect and occasionally resist active attacks from outsiders at the network boundary. This is not surprising because the industry has responded to the customer's perception that the main (if not only) threat to its information systems has been from attackers seeking to penetrate its network from the outside. The industry's historical view has been that the insider threat is mainly a matter of personal trust and network isolation, with the main mitigation to this threat being non-technical: personnel screening complemented with background investigations, information awareness and education, and identity management. Technologies can provide a good degree of security if they are judiciously deployed and carefully maintained (Skoudis, 2009). Users of the U.S. Government network have no expectation of privacy. Nevertheless, there are still problems that exist when it comes to protecting the network. Without continuous monitoring we cannot track down perpetrators without some form of audit trail. So, the lack of logging activity may complicate the defense of the network.

2. Access to information resources can be controlled either through a passive device or through active monitoring. An access control monitor determines whether the actor is authorized to use the resource as requested. If so, access is granted; otherwise it is denied. Before making a decision, the monitor may validate the user through some form of identity management. In many cases, this process of determining authorization is combined with authentication. Possession of a token can imply that the user is someone who has been authorized to obtain access to a particular resource. After making the decision, the monitor may write an audit record to an event log. The audit trail can serve as input to an intrusion detection system that looks for signs of unauthorized activity. It can provide evidence of wrongdoing when such activity is discovered. Access controls serve to enforce an authorization policy, which specifies what activity is allowed and who is allowed to initiate it.

3. More recently, several categories of dedicated insider threat, insider fraud, and data exfiltration mitigation products have begun to emerge in the government network and are characterized as advancing the state-of-the-art in insider threat mitigation. Although many of these products are Intrusion Detection Systems (IDS) like technologies focused inward, the trend is now toward products that focus on host-level activities, including behavior profiling to help differentiate between accidental misuse and true malicious insider activities. Some products also examine behavior profiles that help identify the passive insider. Numerous patent applications and patents for larger security technologies also include anti-insider threat elements. At least one technology dedicated to insider threat mitigation has been patented (Tavani and Moor, 2001).

RECOMMENDATION

1. In the most restrictive environments, authorization policies are based on the principle of confinement, widely known as least privilege or “need to know”. An information resource is kept within its domain of intended operation and made available only to persons and processes that need it to fulfill the mission served by the resource. To everyone and everything else, it is either invisible or out of reach. Confinement though does not mean that information is kept from people who can use it in fulfillment of an organization’s mission. Doing so would be a breach of availability, which arguably is the most important element of information security. Confinement only means that people and computer processes are denied access to information resources unless there is a reason to do otherwise. It limits the trust that has to be placed in users and the software that they use. A related principle is that of limiting access rights of any single individual. By partitioning duty responsibilities, and corresponding authorizations, the damage that any one individual can inflict can be controlled. Many authorization policies are based on classifications, which are used to label information. These markings impose access and handling restrictions on the information. Markings in turn correspond to assigned security clearances, which are assigned to users and processes. Together, they may determine whether a user or process can access a particular resource. Though continuous monitoring has been “required” of agencies for several years, many lacked the inventory knowledge of their own systems to be able to implement continuous monitoring effectively.

2. Achieving continuous monitoring requires a balanced combination of processes, people, and technologies to help organizations automatically detect, report, and correct vulnerabilities in their IT environments. Human judgment is essential for sound cyber security assessments and monitoring. But automation tools can also streamline processes and help eliminate errors and oversights. Continuous monitoring is a critical activity in assessing an organization’s

information security posture. Cyber security professionals also realize an effective continuous monitoring program must adapt to the ever changing technology and cyber security threat landscape.

1. Although profiling is not an accurate science, it can prove to be an important tool in identifying insider threats before an attack. Continuous monitoring is necessary to establish logs; lack of logs complicates the defense posture. Audit trails can serve as inputs to an IDS that looks for signs of unauthorized activity. The use of honey tokens can provide some level of detection, providing a mechanism for detecting that an attack occurred. Rather than detecting or monitoring actual events, this passive user profiling allows an organization to identify potential insiders for further actions. One of the greatest misconceptions of honey pots are they have to be a computer; some physical resource for the attacker to interact with. While this is the traditional manifestation of honey pots, it's not the only one. A honey token is just like a honey pot, you put it out there and no one should interact with it. Any interaction with a honey token most likely represents unauthorized or malicious activity. What you use as a honey token, and how you use it, is up to you.

2. Another example is bogus Social Security Numbers (SSN) or bogus credit card numbers. We have read numerous stories of large databases being compromised, with thousands of SSNs or millions of credit card numbers compromised. Even worse, often these compromises are not detected until weeks if not months later. This gives attackers an extensive amount of time to use or sell the information. Honey tokens can once again be used to simplify this problem. Bogus numbers can be embedded in a database. If the numbers are accessed, you know someone is violating system security. A university could put SSN honey tokens in their student database. If someone attempted to steal the entire database (as has happened at several universities) the attackers would also be grabbing the honey tokens mixed with the valid SSNs. The same could be done for credit card numbers embedded into a vendor's on-line ecommerce site. These honey tokens would be unique numbers, so attackers would not know what the honey token was and what valid numbers were. Databases could watch for whenever someone attempted to access the records and generate an alert. Or, IDS sensors could be configured to watch the local networks. If these honey token numbers are detected on the wire, then the databases have most likely been compromised.

3. Just like traditional honey pots, honey tokens do not solve a specific problem. They are not designed specifically to detect or prevent attacks. Instead, they are a highly flexible and simple tool with multiple applications to security, everything from detection to identifying who your threat is and their motives. The honey tokens' value lies in their simplicity. You deploy a digital file or record and if anyone accesses them, you potentially have a problem. Honey tokens can be used primarily for the insider threat, from the trusted individuals on the inside. You leverage the fact that the insider attacker knows your internal environment and has access to files, information and records (including the honey tokens) that untrusted outsiders would not have access to. Also, this paper asserts that honey tokens should not be used by themselves. As is true with almost any technology, their real value is when they are combined with other solutions. For example, in many cases honey tokens may not prove unauthorized activity. Instead, they may merely indicate you have non-conforming behavior. You most likely will have to use other tools to confirm if someone is acting with malicious intent. This is accomplished with continuous

monitoring. Honey tokens are an exciting new dimension for honey pots, especially for the insider threat. They are cost-effective, simple to deploy, and highly-effective. Honey tokens represent an entirely new field for honey pot concepts; expect to see much more development in this area.

COUNTERARGUMENT

Attackers cannot be banned even when known. Filtering or content-based censorship is impractical sometimes because it seems to be laborious. Also so many privacy issues continue to be on the rise, especially with the issue of identity theft. People are more concerned now than before about the personally identifiable information (PII). No PII inventory or catalog can be adequate or complete without a sufficiently broad understanding of what personal information should be considered identifiable. A common misconception is that PII only includes data that can be used to directly identify or contact an individual (e.g., name, email address), or personal data that is especially sensitive (e.g., Social Security number, bank account number). Human adversaries adapt to filtering. Data elements that may not identify an individual directly (e.g., age, height, birth date) may nonetheless constitute PII if those data elements can be combined, with or without additional data, to identify an individual. In other words, if the data are linked or can be linked ("linkable") to the specific individual, it is potentially PII.

Another counterargument is that content filters may block legitimate use (goal of attack). Often too much human effort is exercised to review all messages and becomes laborious and tendencies exist to reduce our security posture.

CONCLUSION

Personal attitudes continue to be a factor in technology development. Increasing concerns over privacy rights as more and more personal data is being collected and stored online has led to fear that the government is watching them, making vendors reluctant to develop, and organizations to adopt, the kinds of user-monitoring capabilities needed to detect malicious insider activity. Continuous monitoring is a necessary evil to protect the network. Much insider threat research points toward social and behavioral characteristics as reliable indicators of a potential for network abuse.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

Auerbach, Dan. *Do Not Track: Are Weak Protections Worse Than None At All?* May 14, 2013. https://www.eff.org/deeplinks/2013/05/how-weak-current-dnt-proposal (accessed May 14, 2013).

Corcos, Christine. *Internet Privacy Research.* October 14, 2004. http://faculty.law.lsu.edu/ccorcos/Internetprivacypage.htm (accessed May 7, 2013).

Skoudis, Edward. "Information Security Issues in Cyberspace." In *Cyberpower and National Security*, by Stuart H. Strarr and Larry K. Wentz, 171-205. Washington, D.C.: National Defense University Press, 2009.

Tavani, Herman T., and James H. Moor. "Privacy Protection, Control of Information, and Privacy- Enhancing Technologies." *ACM Digital Library SIGCAS Computers and Society*, 2001.

Walters, Gregory. "Privacy and Security: An Ethical Analysis." *ACM Digital Library SIGCAS Computers and Society*, 2001.

Recommendations for U.S. Cyber Command

Major Christopher T. Rubiano, U.S. Air Force (792d Intelligence Support Squadron)

ABSTRACT

As the United States finds itself growing in dependency on cyberspace, the US Department of Defense (DOD) also finds itself more and more reliant on the cyber operational domain. Given this growing dependency, the pressing need exists for U.S. Cyber Command (USCYBERCOM) to develop cyber capabilities amidst shrinking resource pools. For those naysayers who do not believe a "cyberwar" can have significant impacts, one need only look at the 2007 cyber-attacks on the Baltic country of Estonia, a country analogously dependent on cyberspace just like the United States. Having faced its watershed event, Estonia has implemented a creative initiative since 2007 known as its Cyber Defense League, which amounts to a volunteer civilian organization that would assist its military in the event of a national cyber emergency. Along these lines, this paper recommends the DOD pursue a similar domestic initiative to leverage civilian capabilities in times of national emergency, a concept not too different from the Civil Reserve Air Fleet (CRAF). Additionally, in keeping with national-level strategy to build partner capacity, the DOD should focus resources on developing international cyber capabilities just as much as it has focused on developing airlift capabilities, as an example. Now, one might offer the counterargument that the culture in the U.S. is just not the same as in Estonia and therefore a Cyber Defense League will be too difficult to establish. However, this paper will advocate an approach that USCYBERCOM can take a lesson from "Google" to address such cultural obstacles.

DESCRIPTION OF ISSUE

1. A significant strategic issue facing the U.S. Department of Defense (DOD) today is how best to assure mission continuity in cyberspace despite a likely flat-line to shrinking financial resources, reduced manpower, and all the more increasing reliance on civilian networks, not only by the U.S. but also by its allies, coupled with growing threats originating from nation-state actors to everyday cyber criminals. The DOD, through USCYBERCOM, must not maintain the status quo and focus only on developing organic capabilities; in fact, given a resource-constrained environment, it may not have a choice other than to look for creative ways to leverage resources in the civilian sector as well as in allied or partner nations.

2. Among the country's strategic challenges, the U.S. government faces some serious financial challenges in the foreseeable future which, in turn, have affected the DOD's fiscal plans. These challenges include a growing national debt, recovery from a recession with unemployment rates hovering near 9%, and rising costs in healthcare which can cut into overall discretionary spending to include defense spending. Given these fiscal pressures, the Secretary of Defense (SECDEF) has put added emphasis on the military services to pursue prudent spending and search for added efficiencies. In fact, last year, SECDEF directed the military services to "find at least $100 billion in savings" over five years as well as announced initiatives aimed at cutting $54 billion in overhead costs particularly in headquarters and support bureaucracies.[1] Somewhat surprisingly, given the increased attention on cyberspace, even the DOD's IT infrastructure was not off the SECDEF's scope of targeted efficiencies with planned enterprise-level consolidations expected to yield about $1 billion in savings per year.[2] Overall, the current DOD budget will barely keep pace with inflation in the next two fiscal years with reduced to zero real growth in the

out years.[3] Bottom line, fiscal pressures on the DOD will likely translate to fiscal pressures on all its organizations to include USCYBERCOM.

3. Such fiscal pressures correlate with DOD manpower reductions or caps at best. As part of the SECDEF's plan, the Army and Marines Corps would be cut by as many as 47,000 troops starting in FY15, in conjunction with the planned drawdown in Afghanistan.[4] Additionally, the USAF will remain capped at an active duty end strength of 332,800, a number it is trying to reach by the end of FY12 by cutting excess through Force Shaping programs.[5] So, at least from a military manpower perspective, growth across the DOD does not appear to be in future plans.

4. While budgets and manpower may be shrinking in the next few years, an inverse relationship seems to exist with regard to the DOD's increasing reliance on cyberspace. Additionally, as highlighted in the President's latest National Security Strategy, among the threats in our strategic environment, "The space and cyberspace capabilities that power our daily lives and military operations are vulnerable to disruption and attack."[6] Arguably, the growing reliance and vulnerability have played a major role in the standup of USCYBERCOM. Similarly, our Allies recognize the immediate importance of charting the proper course ahead for operating in the cyber domain. For example, cyber defense has garnered much attention as NATO attempts to redefine itself in its new Strategic Concept. But what's even more eye- opening is the fact that the lines between civilian and military networks grow blurrier by the day. In fact, Harvard Law Professor Jack Goldsmith noted that "[n]inety to 95 percent of U.S. military and intelligence communications travel over private networks."[7] With these challenges in mind, USCYBERCOM has the opportunity to explore some creative options to address these challenges, particularly while still in its infancy.

RECOMMENDATION

1. USCYBERCOM can explore the following options:
    a. Consider leveraging the civilian sector in a relationship or organization similar to the airlift community's Civil Reserve Air Fleet
    b. Pursue an international consortium similar to the successful 12-nation C-17 Heavy Airlift Wing under NATO's Strategic Airlift Capability.

These options build upon the National Security Strategy tenets to engage the domestic civilian sector as well as the international community given shared challenges particularly in cyberspace and to spread the burden given resource constraints felt among the U.S. and its Allies.[8]

2. USCYBERCOM can take a lesson from two existing, successful initiatives. The first is the Civil Reserve Air Fleet (CRAF). Per a USAF fact sheet, the CRAF is described as, "Selected aircraft from U.S. airlines, contractually committed to CRAF, support Department of Defense airlift requirements in emergencies when the need for airlift exceeds the capability of military aircraft."[9] If the DOD itself can't grow, per say, perhaps part of the solution may be to consider a CRAF-like "Civilian Reserve Cyber Force" that could be leveraged under similar criteria of national emergencies, but could also build on the linkage between civilian and military networks (i.e., the growing dependence of the military on civilian networks and private expertise). This model actually follows an initiative the Estonians have already established called the "Cyber Defense League," which the country stood up in the years following the cyber-attacks experienced in April 2007.[10] The Cyber Defense League involves mobilizing volunteer civilian

programmers, computer scientists, and software engineers who would function under a unified military command in wartime, "dedicated to maintaining the country's security and preserving its independence."[11] The importance of this auxiliary force becomes more apparent when one considers how much Estonia relies on cyberspace. To give an idea, "[e]ighty percent of Estonians pay their taxes online and engage in electronic banking."[12] So, when Estonia did get attacked, the impetus was there for its citizens to rally behind its military.

3. Many questions would obviously surround the establishment of such a Civilian Reserve Cyber Force. For example, its role would need to be scoped based on legalities and/or authorities (e.g., CND vs. CNA vs. CNE, etc.) Similarly, arguments could be made as to what organization it would report to during times of national emergency, such as DOD (USCYBERCOM) or Department of Homeland Security (DHS) or a combination of the two particularly with critical infrastructure. Also, from a funding standpoint, while CRAF funding is fairly cut and dry with respect to the number of aircraft and crews provided, such criteria may be harder to define with respect to what quantifiable cyber-related products or services could be provided.

4. Along the same lines of leveraging domestic partnerships to address shrinking resource pools despite growing cyberspace concerns, USCYBERCOM can look to work with a geographic Combatant Command such as USEUCOM to take advantage of its strong relationships with NATO Allies and Partner Nations. To address the mutual reliance on cyberspace by the U.S. and its Allies/Partners, a consortium approach could be taken to establish an international Cyber Capabilities Wing, similar to that of the successful C-17 Heavy Airlift Wing (HAW) at Papa Air Base, Hungary, established under the NATO Strategic Airlift Capability initiative.[13] This 12-nation collaborative effort is a model for how multiple countries, each with limited means, can combine together to address shared needs and capability shortfalls. A notional Cyber Capabilities Wing established in this image could build on the HAW's momentum and be a natural fit especially as NATO finds itself trying to redefine its Strategic Concept, with cyber security among the key concerns of all Allies and Partner countries.

5. As with the notional Civil Reserve Cyber Force recommendation, the establishment of a Cyber Capabilities Wing would generate just as many basic questions. For example, under the construct of the HAW, each of the 12 member nations contributes a certain amount of resources based on a pre-agreed number of flight hours a country expects to receive, which corresponds to a fairly quantifiable product. With a consortium-based Cyber Capabilities Wing, the construct may have to be more of a fee-for-service basis, with the service being something like network optimization or Red Team services.

6. With regard to the recommendation to establish the Civilian Reserve Cyber Force in the model of Estonia's Cyber Defense League, at least one cyber expert feels there is something inherent to Estonia's history and culture that makes that initiative possible, whereas in the U.S., the culture may be more prohibitive. According to Stewart Baker, who worked under the Department of Homeland Security during President George W. Bush's administration and was a former general counsel at the National Security Agency, such an organization "would have been helpful," however, the same kind of relationship as Estonia currently has does not exist between the U.S. public and private sectors. Baker describes the relationship in the U.S. as:

> "The people who work in IT in the U.S. tend to be quite suspicious of government. Maybe they think that they're so much smarter than governments that they'll be able to handle an attack on their own. But there's a standoffishness that makes it much harder to have that kind of easy confidence that you can call on people in an emergency and that they'll respond."[14]

Again, given Estonia's history of being under Russian control and experiencing a watershed cyber-attack of sorts, there was a natural feeling of patriotism to draw upon in its citizens. If the cultural difference in the U.S. private sector is true as Baker describes, then perhaps a "9-11" style cyber-attack may be required as the impetus for a Civilian Reserve Cyber Force.

COUNTERARGUMENT

As a counterargument, however, two authors take the approach that USCYBERCOM, being in its infancy, has the opportunity to address this public-private cultural divide by molding itself with innovative approaches.[15] One such approach is to build the organization with a culture like the popular company Google, which attracts people to work there and inspires creativity and innovation. The authors argue that "cyber warriors deserve equally tech-savvy leaders who understand and appreciate their accomplishments, empower creative problem solving, encourage out of the box thinking who can empower individual efforts and yet successfully focus these efforts into a cohesive team; we believe Cyber Command should be up to this task."[16] With such a culture, the authors argue that Cyber Command could be looked at similar to how U.S. Special Forces is seen as an elite and highly respected organization. Thus, cyber-savvy individuals would be attracted to working for Cyber Command in the same way they are attracted to companies like Google.

CONCLUSION

In conclusion, the DOD faces some daunting strategic challenges including fiscal and manpower shortfalls which make addressing its growing reliance and the increasing number of threats in cyberspace all the more difficult. With the recent establishment of USCYBERCOM, the DOD has the opportunity to creatively mold this organization so that it can effectively address these challenges. Two such ways USCYBERCOM can approach burden sharing while improving domestic public-private relationships as well as international relationships is through pursuing a Civil Reserve Cyber Force, similar to the Civil Reserve Air Fleet, and leading the development of a multi-national consortium Cyber Capabilities Wing, similar to the idea behind the 12-nation Heavy Airlift Wing under the NATO Strategic Airlift Capability initiative.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. SECDEF Speech on "Statement on Department Budget and Efficiencies," p. 1.
2. SECDEF Speech on "Statement on Department Budget and Efficiencies," p. 2.
3. SECDEF Speech on "Statement on Department Budget and Efficiencies," p. 6.
4. SECDEF Speech on "Statement on Department Budget and Efficiencies," p. 6.
5. FY2012 AF Posture Statement, p. 6.
6. *US National Security Strategy*, p. 8.
7. Gjelten, "Extending the Law of War to Cyberspace," p. 2.

8. *US National Security Strategy*, p 28.
9. "USAF Fact Sheet: Civil Reserve Air Fleet," p. 1.
10. Gjelten, "Volunteer Cyber Army Emerges in Estonia," p. 1.
11. Ibid.
12. Ibid.
13. "NATO Topic: Strategic Airlift Capability," p. 1.
14. Gjelten, "Volunteer Cyber Army Emerges in Estonia," p. 2.
15. Conti and Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," p. 3.
16. Conti and Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," p. 6.

BIBLIOGRAPHY

Conti, Gregory and Jen Easterly. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *smallwarsjournal.com*, 29 July 2010. http://www.smallwarsjournal.com

Department of the Air Force. *Presentation to the Committee on Armed Services, United States House of Representatives, Fiscal Year 2012 Air Force Posture Statement on 24 February 2011*, Washington, DC: SECAF, 24 February 2011.

Gjelten, Tom. "Volunteer Cyber Army Emerges in Estonia," *NPR.org*, 24 January 2011. http://www.npr.org

"NATO Topic: Strategic Airlift Capability". http://www.nato.int

"USAF Fact Sheet: Civil Reserve Air Fleet," http://www.af.mil

U.S. Office of the President of the United States. *National Security Strategy*, Washington, DC: The White House, May 2010. http://www.whitehouse.gov/ (accessed 9 March 2011).

U.S. Office of the Secretary of Defense. "Statement on Department Budget and Efficiencies," Washington, DC: SECDEF, 6 January 2011. http://www.defense.gov

Mission Assurance: Continuity of Operations Guidance and Recommendations for Application to Cyber

Mr. Brian Hale, U.S. Air Force (AFIT)

ABSTRACT

Military organizations have embedded information technology (IT) into their core mission processes as a means to increase operational efficiency, improve decision-making quality, and shorten the sensor-to-shooter cycle. This IT-to-mission dependence can place an organization's mission at risk when an information incident (e.g., the loss or manipulation of a critical information resource) occurs. Non-military organizations typically address this type of IT risk through an introspective, enterprise-wide focused risk management program that continuously identifies, prioritizes, and documents risks so an economical set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level. The explicit valuation of information resources in terms of their ability to support an organization's mission objectives provides transparency and enables the creation of a continuity of operations plan and an incident recovery plan. While this type of planning has proven successful in static environments, military missions often involve dynamically changing, time-sensitive, complex, coordinated operations involving multiple organizational entities. As a consequence, risk mitigation efforts tend to be localized to each organizational entity making the enterprise-wide risk management approach to mission assurance infeasible. This paper identifies cyber-related continuity of operations recommendations to help establish the underlying guidance required to ultimately support mission assurance; and more specifically, the timeliness and relevance of notification following an information incident.

DESCRIPTION OF ISSUE

1. Background. Information has become the critical asset in the operation and management of virtually all modern organizations.[1, 5 13, 14, 35, 37] Organizations continue to embed IT into their core mission processes as a means to increase their operational efficiency, exploit automation, reduce response time, improve decision quality, minimize costs, and/or maximize investments.[6, 7, 15, 39] This is especially true in military environments where information is constantly being collected, processed, analyzed, distributed, and aggregated to support situational awareness, operations planning, intelligence, and command decision making.[18] However, the increasing dependence upon information and IT to produce value within the organization has resulted in an environment where an information incident (e.g., the loss or degradation of the confidentiality, availability, integrity, non-repudiation, and/or authenticity of an information resource or information flow) can result in significant mission degradation or failure.[9, 21-23, 30, 41] When this incident occurs, the decision makers within organizations whose mission is critically dependent upon the affected information must be notified in a timely manner so they may take appropriate contingency actions.

2. Organizations typically employ an enterprise-wide focused risk management program that identifies and prioritizes risks so a set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level given a limited budget.[11-12, 26-29, 33, 36] Risk management has proven successful in static environments, when all stakeholders participate, and all resources critical to the success of the operations can be enumerated. However, military missions often involve dynamically changing, distributed, time-sensitive, complex, cooperative, and coordinated operations involving multiple organizational units

within a military service (e.g., fighter squadrons, aerial refueling squadrons, special operations units), between various service elements (e.g., Army, Navy, Air Force, Marines), between various national agencies, and across multiple allied coalition partners.[8] Because each organization participating in the mission is resourced and managed as a separate entity, a centralized enterprise-wide risk management approach is largely infeasible. Since the accuracy, conciseness, and timeliness of the information used in decision-making processes dramatically impacts the quality of command decisions, and hence the operational mission outcome, the recognition, quantification, and documentation of critical information dependencies is essential for the organization to gain a true appreciation of its operational risk.[16, 24, 38] By explicitly documenting information dependencies and formalizing the linkage between mission operations and the underlying dependent information resources, mission commanders and their staff can maintain awareness of their critical information resources during mission operations and ultimately, improve situational awareness. When an information incident occurs, the incident notification can recall and display context-dependent information collected when documenting the linkage between information dependencies and mission operations, to include potential contingency measures, therefore, aiding continuity of operations.

3. Issue Significance. In 1996, eight national critical infrastructures were specified in Presidential Executive Order 13010 as being so vital that their "incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[20] One of the centers of gravity included was the continuity of government. The threats to the critical infrastructures were classified into two categories: physical and cyber threats.[20] Cyber threats continue to escalate and cyberspace has grown to be a contested domain.[10] Simultaneously, the mission dependency on cyber assets continue to rise.[31-32] Coupling the expanding threats and cyber dependencies increases the potential for cyber-related risks to potentially disrupt operations. The recently declassified 2010 Comprehensive National Cybersecurity Initiative (CNCI) identifies cybersecurity as one of the most serious economic and national security challenges the United States faces, and that the nation is inadequately prepared to deal with these challenges.[19] The acknowledged importance of mission to cyberspace dependence is further identified in the United States Air Force Blueprint for Cyberspace. One of the objectives stated in the blueprint is "to ensure mission success by maximizing cyber continuity, availability, and resilience."[2] This speaks to the seriousness and noted contested nature of cyberspace. However, initiatives such as improved cyberspace situational awareness, security, and information assurance efforts across the cyber infrastructure may elevate resiliency and improve operational capabilities.

4. To ensure Defense Critical Infrastructure (DCI) availability, to include cyber-related infrastructure, the Department of Defense (DOD) uses the DCI Program (DCIP), a risk management program.[17] It is DOD policy to conduct assessments of the threats and hazards, vulnerability, and risk to DOD-owned DCI and the inter- and intra-dependencies needed to accomplish required DOD missions, with the support of the appropriate DOD Components and Defense Infrastructure Sector Lead Agents. These activities are the major elements of the DCIP and the actions should support incident management. Also, the DCIP must coequally complement other DOD programs, functions, and activities contributing to mission assurance through risk management.[16]

5. Furthermore, the 2010 Quadrennial Defense Review (QDR) report recognized risk management as central to effective decision-making and is vital to mission success, although it can be challenging to accomplish. The QDR noted the need for non-quantitative methods (informed judgments, expert opinions, and scenarios) to improve the military complexity associated with the identification, categorization, and aggregation of operational risk.[38] Recognizing the increasingly contested nature of cyberspace, the need to enhance awareness of cyber dependencies, and the need for non-quantitative risk assessment measures, recommendations to improve cyber-related continuity of operations are detailed next.

RECOMMENDATION

1. At least since the Cold War era, government organizations have had a requirement to continuously conduct their operations, regardless of any disruptions the organizations may face. However, recent events such as the terrorist attacks of 11 September 2001 against the United States and the cyber-attacks against Estonia have reemphasized the need to ensure continuity of operations after a disaster or extended disruption. All organizations should be prepared to respond to a wide range of potential emergencies. To this end, the author recently conducted a content analysis of 61 United States (US) Government and non-US Government publications to investigate the current continuity of operations policy landscape.[25] The publications were reviewed for such concepts as mission, assurance, assessment, planning, continuity, crisis, emergency, disruption, disaster, impact, incident, threat, scenario, organizational resilience, infrastructure protection, vulnerability, and risk.

2. U.S. Government publications included DOD and Air Force issuances and policies, and documents developed by the National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce. Non-US government documents included International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) documents, IT Infrastructure Library (ITIL) documents developed by the United Kingdom Office of Government Commerce, the IT Governance Institute's (ITGI) Control Objectives for Information and related Technology document, and the Operationally Critical Threat, Asset, and Vulnerability Evaluation criteria document (Carnegie Mellon University). Based on the author's content analysis,[25] the following five recommendations are proposed:

3. First, the Air Force should produce an overarching continuity of operations plan matrix, or a similar umbrella matrix, linking all of the disaster, contingency, emergency, crisis, etc. plans together. NIST published a similar table in Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems (Draft),* 2009. The following Table provides an excerpt and example of the type of matrix proposed. The Air Force Civil Engineering community did this, in part, within the documents they authored; however, no overarching chart was discovered for all Air Force plans.

Table 1. Types of Plans[34]

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining business operations while recovering from a significant disruption.	Addresses business processes at a lower or expanded level from COOP mission essential functions	Functional continuity plan that may be activated with a COOP to sustain noncritical functions.
Continuity of Operations Plan (COOP)	Provides procedures and guidance to sustain an organization's mission- essential functions at an alternate site for up to 30 days; mandated by federal directives.	Addresses the mission essential functions; facility- based plan; information systems are addressed based only on their support to the mission- essential functions.	Functional continuity plan that may also activate several business unit- level BCPs.
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a system cyber-attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	System contingency plan that may activate an ISCP or DRP, depending on the extent of the attack.

4. Second, in addition to a matrix, an overall continuity management plan should be authored. ITIL recommended, at the highest level, there is a need for an overall coordination plan. The Air Force does have a plan close to what is needed; the plan is the Comprehensive Emergency Management Plan (CEMP) 10-2.[3] The CEMP provides comprehensive guidance for emergency response to physical threats resulting from major accidents, natural disasters, conventional attacks, terrorist attacks, and Chemical, Biological, Radiological and Nuclear attacks. However, the Emergency Management Program does not cover non-physical threats, including cyber threats. As such, the CEMP should be revised to include cyberspace-related emergency management information, or a new, overarching, comprehensive emergency plan should be developed to correlate and synergize all continuity of operations efforts.

5. Third, there is DOD guidance directing the construction of DCI mission focus statements to specify DCI performance standards and conditions necessary for mission success. However, based on the publications analyzed, there appears to be lack of guidance on how to implement the guidance. If the standards can be specified though, they should be able to be measured and contribute to mission metrics.

6. Fourth, the data discovered during the content analysis suggested there is a general absence of preparedness policy authored by the communication and information (cyber) community. With the previously stated importance of IT resources and assets, cyber preparedness guidance needs to be published to help ensure continuity of operations and assure mission success. For example, communications are sometimes considered in contingency plans; however, typically from a long- established standpoint of command and control communications (e.g., telephones, radios, faxes, and mass notification systems). The plans focused on communication-out procedures, such as using runners, flags, or flares, not on how information technology may be imbedded within critical processes and the true impact of disrupting communications.

7. Lastly, and while this assertion needs to be supported empirically, anecdotally it appears from the author's 24 years of experience in the Air Force that the Air Force's Operational Risk Management (ORM) program is basically equated to as a safety mishap prevention program. Although ORM may be useful in preventing mishaps, ORM can be applied beyond safety. Some of this safety bias is shown in the principle ORM publication (AFPAM 90-902, *Operational Risk Management Guidelines and Tools*, 2000), as it discussed "mishap prevention," "safeguarding health and welfare," and "record low mishap rates." However, AFPAM 90-902 did go on to state, "Beyond reducing losses, risk management also provides a logical process to identify and exploit opportunities."[4] Additional education and emphasis should be given as to how ORM should be embedded within operational processes and can be used beyond just mishap prevention.

8. The development of cyber-related continuity of operations guidance should be championed in partnership between the HAF cyber lead and SAF/CIO A6 (Information Dominance and CIO). The lead major command should be Air Force Space Command, with the guidance development conducted by 24th Air Force. Since developing policy and guidance are inherent responsibilities of these management organizations, there should be no additional costs (manpower and funding) associated with developing this continuity of operations guidance.

COUNTERARGUMENT

It could be argued the return on investment for implementing all of the recommendations across all mission areas could be below an acceptable threshold; but, targeted implementations in select mission areas may be plausible and may be very advantageous. Also, the status quo could be disputably maintained since true cyberspace situational awareness may be elusive given the technical, social, and organizational complexity of the challenge. However, as the dependency on IT for mission success continues to grow, cyberspace continues to become an ever increasingly contested domain, and the necessity for cyberspace situational awareness intensifies, incremental steps should be taken to enhance cyberspace situational awareness capabilities.

CONCLUSION

Information technology has been virtually integrated into every mission process. Given the level of dependency on IT to conduct operations, a tiered continuity of operations commitment is needed to enhance cyberspace situational awareness and, more importantly, increase mission assurance. Foundationally, to achieve this end, cyber-related continuity of operations guidance needs to be established to enable mission assurance. The guidance recommendations include authoring an overall Air Force continuity management plan, to encompass an overarching Air Force continuity of operations plan matrix, improving instructions on how to implement Defense

Critical Infrastructure guidance, creating cyber-specific preparedness policy, and embedding operational risk management principles within operational processes. Although the cyber domain is a ubiquitous and complex environment, every attempt must be made to recognize, assess, and react to any information incidents impacting a mission. General Eric Shinseki, former US Army Chief of Staff, once commented, "If you dislike change, you're going to dislike irrelevance even more."[40]

BIBLIOGRAPHY

1. Abrams, Marshall D., Sushil G. Jajodia, and H.J. Podell, eds. *Information Security: An Integrated Collection of Essays.* Los Alamitos, CA: IEEE Computer Society Press, 1995.
2. Air Force Space Command. *The United States Air Force Blueprint for Cyberspace*. Peterson AFB, CO: HQ AFSPC, 2 November 2009.
3. Air Force Instruction (AFI) 10-2501. *Air Force Emergency Management (EM) Program Planning and Operations*, 24 January 2007.
4. Air Force Pamphlet (AFPAM) 90-902. *Operational Risk Management (ORM) Guidelines and Tools*, 14 December 2000. 5.
5. Air Force Policy Document (AFPD) 10-24. *Air Force Critical Infrastructure Program (CIP)*, 28 April 2006.
6. Alberts, David S. *Information age transformation: getting to a 21st century military.* CCRP Publication Series, Command and Control Research Program (CCRP), US Office of the Assistant Secretary of Defense, 2002. http://www.dodccrp.org/files/Alberts_IAT.pdf
7. Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network centric warfare : developing and leveraging information superiority.* CCRP Publication Series, DOD C4ISR Cooperative Research Program, US Office of the Assistant Secretary of Defense, 1999. http://www.dodccrp.org/files/Alberts_NCW.pdf
8. Alberts, David S. and Richard E. Hayes. *Understanding command and control.* CCRP Publication Series, Command and Control Research Program (CCRP), US Office of the Assistant Secretary of Defense, 2006. http://www.dodccrp.org/files/Alberts_UC2.pdf
9. Anderson, E., Joobin Choobineh, and Michael R. Grimaila. "An Enterprise Level Security Requirements Specification Model," Proceedings of the 38th Annual Hawaii International Conference (HICSS 2005). 186-196, January 2005.
10. Baker, Stewart, Shaun Waterman, and George Ivanov. In the Crossfire: Critical Infrastructure in the Age of Cyber War. Santa Clara, CA: McAfee, 2009.
11. Carnegie Mellon University Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). *CERT Coordination Center, Software Engineering Institute,* 2004. http://www.cert.org/octave.
12. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management—integrated Framework*, 2004. http://www.coso.org
13. Davenport, Thomas H. and Laurence Prusak. *Working Knowledge: How Organizations Manage What They Know*. Boston, MA: Harvard Business School Press, 2000.

14. Denning, D. *Information Warfare and Security.* Upper Saddle River, NJ: Pearson Education, Inc., 1999.

15. Department of Defense (DOD) Air ForceV2, Volume 1. *DOD Architecture Framework - Version 2.0: Volume 1: Introduction, Overview, and Concepts Manager's Guide*, 28 May 2009.

16. Department of Defense (DOD) Directive 3020.40. *DOD Policy and Responsibilities for Critical Infrastructure*, 14 January 2010. 17.

17. Department of Defense (DOD) Instruction 3020.45. *Defense Critical Infrastructure Program (DCIP) Management*, 21 April 2008.

18. Department of Defense (DOD) Joint Publication 3-13. *Information Operations*, 13 February 2006.

19. Executive Office of the President. *The Comprehensive National Cybersecurity Initiative*. Washington: Executive Office of the President of the United States of America, 3 March 2010. http://www.whitehouse.gov/sites/default/files/Cybersecurity.pdf

20. Executive Order 13010. Critical Infrastructure Protection, 15 July 1996.

21. Fortson, Larry W. and Michael R. Grimaila. "*Development of a Defensive Cyber Damage Assessment Framework*," Proceedings of the 2007 International Conference on Information Warfare and Security (ICIW 2007). Monterey, CA: Naval Postgraduate School, 2007.

22. General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Chapter Report. Washington: United States General Accounting Office, 1996.

23. Grimaila, Michael R. and Larry W. Fortson. "*Towards an Information Asset-Based Defensive Cyber Damage Assessment Process*," Proceedings of the 2007 IEEE Computational Intelligence for Security and Defense Applications (CISDA 2007). 206-212. Honolulu, HI, 2007.

24. Grimaila, Michael R., Larry W. Fortson, and J.L. Sutton. "*Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process*," *Proceedings of the 2009 International Conference on Security and Management (SAM09)*, Las Vegas, NV, 2009.

25. Hale, Brian L. *Mission Assurance—A Review of Continuity of Operations Guidance for Application to Cyber Incident Mission Impact Assessment (CIMIA).* MS thesis, AFIT/GIR/ENV/10-J01. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, June 2010.

26. International Information Security Foundation (I^2SF). *Generally Accepted System Security Principles (GASSP)*, 2005. http://web.mit.edu/security/www/gassp2.html.

27. International Information System Security Certification Consortium, Inc $(ISC)^2$. *Common Body of Knowledge (CBK),* 2009. http://www.isc2.org/cgi-bin/content.cgi?category=8.

28. Information Systems Security Association (ISSA). Generally Accepted Information Security PrinciplesV3.0 (GAISP), 2005. http://www.issa.org/gaisp/_pdfs/v30.pdf.

29. Information Technology Governance Institute (ITGI) COBIT v4.1. Control Objectives for Information and related Technology, 2007. http://www.isaca.org/cobit.

30. Jajodia, Sushil, Paul Ammann, and Catherine D. McCollum. Surviving Information Warfare Attacks. IEEE Computer, 32(4), 57-63 (1999).

31. Lyle, Amaani. "Air Force leaders speak at 2009 Global Warfare Symposium." US Air Force News, 20 November 2009. http://www.af.mil/news/story.asp?storyID=123178818.

32. Millette, Christine D. "Air Force officials to implement hand-held device changes." US Air Force News, 17 March 2010. http://www.af.mil/news/story.asp?storyID=123195331

33. National Institute of Standards and Technology (NIST) Special Publication 800-30. Risk Management Guide for Information Technology Systems, March 2008.

34. National Institute of Standards and Technology (NIST) Special Publication 800-34, Revision 1. Contingency Planning Guide for Federal Information Systems (Draft), October 2009.

35. National Institute of Standards and Technology (NIST) Special Publication 800-60V1, Revision 1. Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

36. Petrocelli, Tom D. Data Protection and Information Lifecycle Management. Upper Saddle River, New Jersey: Pearson Education, Inc., 2005.

37. Pipkin, Donald L. Information Security Protecting the Global Enterprise. Hewlett-Packard Company Professional Books, 2000.

38. Quadrennial Defense Review. "Quadrennial Defense Review Report," United States Department of Defense, February 2010.

39. Rubin, Howard A. Return on IT: The Holy Grail of the Business Value of IT. Wall Street and Technology, 28(2), 15 (2010).

40. Singer, P. W. Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Press; New York, NY, 2009.

41. Ware, Willis H. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security. The RAND Corporation, Santa Monica, CA; February 1970.

Deterring Cyber War: A Cold War Perspective
Major Hector Jimenez, U.S. Air Force (USSOUTHCOM)

ABSTRACT

Ever since the Treaty of Westphalia ended the Thirty Years War in 1648 there have been numerous international agreements to prevent hostilities between sovereign states. Most famous of these treaties is the Kellogg-Briand Pact (Pact of Paris) 1928 in which signatories of the treaty agreed not to resort to war to resolve disputes. Ironically however, within 14 years of this treaty major signatories (e.g. United States, France, and Germany) were already at war with each other. These treaties were founded on the lessons of war and the importance of diplomacy. After World War II, world leaders attempted to create an international system to promote peace. The result was the United Nations and its founding document the U.N. Charter. Article 2(4) of the U.N. Charter states that member states shall refrain in their international relations from the threat or use of force against other member states. Additionally, Article 51 of the Charter recognizes the international right of self-defense against use of force. Implicit in the question of whether and how a nation can respond to a computer network attack is whether the attack constitutes a use of force. The concept of a computer encompasses more than a simple desktop or laptop; it also includes the devices that control much of our critical infrastructure and key resources (e.g. power grids, water mains, and cellular and telephone networks). The potential for widespread damage from a cyber-attack grows in tandem with the growth of systems controlled by computers. What law governs these attacks? Some have referred to these and similar attacks as cyber-warfare, suggesting that the law of war might apply. Yet some scholars argue these attacks look little like the conventional warfare. And if cyber attacks are a form of conventional warfare, does that mean that victims of such attacks might claim the right to use conventional force in self-defense? The writer will advocate that not only are cyber attacks equivalent to armed attacks they also present a national security threat at a global scale, therefore it is time the U.S. takes a proactive step towards addressing these challenges via a Cold War strategy.

DESCRIPTION OF ISSUE

1. According to Jensen (2002), a computer network attack (CNA) falls under three categories: (a) an action below the threshold of use of force, (b) an action equivalent to use of force but short of armed attack, and (c) an action equivalent to armed attack. He argued that traditional weapons systems could easily be classified under one of these categories, but that CNA challenged the prevailing paradigm of warfare, “A CNA may be as benign as preventing a website from functioning properly or as serious as hampering public transportation or causing civilian deaths” (p. 222). A key principle of war limiting the doctrine of self-defense is Jus ad bellum (i.e. necessity), therefore a significant issue facing the Department of Defense (DOD) today is how to apply this principle in response to cyber warfare such as CNA. In their paper, Hathaway et al. (2012) asked what law governs the right to self-defense in response to a cyber attack? In an attempt to answer the question they cited Article 2(4) of the United Nations Charter which states that member states, “shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations” (p. 27). However, they noted that the exception to this rule is found in article 51 which states that “[n]othing in the present Charter shall impair the inherent right of an individual or collective to self-defence if an armed attack occurs” (p. 30). Hathaway et al. argued that Jus ad Bellum may not apply to cyber war because in most cases these activities are done behind closed doors, using non-kinetic means, and through

non-state actors. In other words, these activities are done in secret, using non-lethal measures, and with the help of ambiguous perpetrators. For this reason Hathaway et al. argued that it would be very difficult to apply Jus ad Bellum to cyber war and to prove that that a cyber attack met the United Nations requirements for an attack. Furthermore, Article 4 of the NATO treaty states that a cyber attack, "will not constitute an armed attack that obligates member states to assist one another under Article 5 of the treaty" (Hathaway et al. 2012, p. 33).

2. In support of these views, experts in the field of cyber war (e.g. Graham, 2010, Mudrinich, 2012; Sterner, 2011) noted that attributing a cyber attack to a specific actor is difficult. In other words, even if the attack could be traced to a specific server, attributing the attack to a specific actor could prove impossible given the anonymity of the technology involved. For these reasons, victims of cyber attacks have historically resorted to passive measures such as requesting that the local government from which attacks originated to investigate and prosecute (Graham). However, according to his findings most major world governments have showed little interest in policing these attacks. Sterner made an even more compelling point, "…if the cyber attacker is not a nation-state, retaliation may involve impinging on the sovereignty of the country in which the cyber attacker is physically located or of the country(ies) through which the attack was launched" (p. 66).

3. Another principle of war limiting the right of self-defense is Jus in bello (i.e. proportionality). In other words, any response to a cyber attack must fit the severity of the crime. As stated earlier, the principle of necessity requires that force must be used only as a last resort, when diplomacy is exhausted. According to the literature, proportionality extends this logic, "prohibiting force if the overall scope and intensity of force is excessive in relation to the state's actual or imminent danger. The United States has acknowledged that these principles apply to military responses to cyber-attacks" (Hathaway et al., 2012, p. 36). However, Hathaway et al. cited that applying this principle to cyber war is difficult given the nature of cyber. In conducting warfare military planners must calculate the collateral damage to both civilian life and property against the benefit of achieving the military objective, therefore Hathaway et al. argued that, "due to the nature of harm they inflict, the proportionality of cyber-attacks poses unique challenges" (p. 38).

4. In support of these views, experts in the field of cyber war (e.g. Graham, 2010; Libicki, 2009; Sterner, 2011) have argued that even with all the right planning, the principle of proportionality with respect to self-defense is difficult to meet. Graham noted that, "…the extent of the damage that actually occurs when a state employs such defenses, particularly in relation to innocent systems located in third states, may likely be viewed as violations of both the principles of distinction and proportionality and thus violations of the LOW" (p. 100). Sterner made an even more compelling point, "…it can be argued that the prospect of taking life in a kinetic attack far outweighs the damage one can commit with a cyber attack; that is, it is disproportional" (p. 72). Libicki echoed the same sentiment, "…with cyber-retaliation, the stakes in getting it right are higher, and the arguments about proportionality may surface only after it is too late to take things back" (p. 68).

5. With these challenges in mind, U.S. policy makers have the opportunity to implement a radical new strategy to address these challenges, particularly since cyber is the new frontier where tomorrow's wars will take place.

RECOMMENDATION

1. Ever since the Treaty of Westphalia ended the Thirty Years War in 1648 there have been numerous international agreements to prevent hostilities between sovereign states. According to Jensen (2002), the most famous of these treaties is the Kellogg-Briand Pact (Pact of Paris) 1928 in which signatories of the treaty agreed not to resort to war to resolve disputes. Ironically, he noted that within 14 years of this treaty major signatories (e.g. United States, France, and Germany) were already at war with each other, "these treaties were founded on the lessons of war and the importance of diplomacy" (p. 215). Despite the shortcoming of the Pact of Paris, U.S. policy makers should consider employing a cyber treaty similar to the Pact of Paris. This treaty would enforce diplomacy for dealing with any cyber attacks on any signatory of the treaty, thereby deterring conventional warfare. According to scholars (Hoskins, Liu, & Relkuntwar, 2005; Libicki, 2009; Mudrinich, 2012) the way to overcome the challenges of Jus ad bellum is to improve our international relationships with our allies. For this reason, Hoskins et al. argued that when an attack occurs it is in the best interest of the victim to consult with all players and determine a course of action. In other words, bilateral action is better than unilateral action in any cyber retaliatory decision. In their words, "one should launch a counterattack because it is the best option, not because it is the only one available" (p. 22). Mudrinich argued that cyber is a global domain and not just resident to the United States, "Almost a third of the world's population uses the Internet and there are more than four billion digital wireless devices in the world" (p. 185). Therefore, he emphasized international cooperation with our allies to improve policing of cyber attacks. He also believed that international cooperation (i.e. bilateral) would evolve to collective self-defense and collective deterrence. Libicki echoed the same sentiment and noted that unilateral actions in cyberspace were counterproductive. He believed that in order to succeed in cyberspace coalitions were essential, "…the more easily information flows among coalition members, the more easily they can coordinate action. The strengths of one partner can cover the gaps of another" (p. 152).

2. In order to deal with the challenges of attribution and proportionality (i.e. Jus in bello) U.S. policy makers should consider the nuclear deterrence strategy employed during the Cold War. Some scholars (e.g. Beidleman, 2009; Sterner, 2011) have argued that employing this policy of deterrence is the best course of action to take. They believe that by letting our enemies know up front what they stand to lose can be an effective strategy and could ultimately save the government billions of dollars in defense costs. In other words, deterring aggression relieves the defender from spending on defense. Sterner argued that a good cyber deterrence strategy could be developed using Israeli strategy. He noted that Israel continuously seeks to deter attacks by changing the nature of war. For example, Sterner emphasized that Israelis successfully countered cross-border Palestinian raids, "by threatening and conducting retaliatory attacks against Jordan and Egypt, each of which had greater reason to fear Israeli retaliatory threats and possessed capabilities to threaten and punish Palestinian raiders" (p. 70). Beidleman echoed the same sentiment and argued that offensive capabilities offer the best deterrence, "offensive cyber capabilities and operations provide a state the means and ways for retaliation and enhance the perceived probability that aggressors will pay severely for their actions" (p. 17). Additionally, he argued that both offensive and defensive capabilities play a critical role in deterrence. With

respect to defensive cyber capabilities, Beidleman noted that not only do they secure critical infrastructure and key resources, but they also degrade the advantage to the aggressor. In other words, "defensive cyber capabilities increase a state's resistance to attacks and reduce the consequences of attacks" (p. 18).

COUNTERARGUMENT

1. With regard to the recommendation for strengthening international relationships and diplomacy in combating cyber attacks similar to the Pact of Paris, at least one scholar (e.g. Schmitt, 1999) believed that cyber attacks do not constitute use of force as noted in the U.N. Charter, therefore a right to self-defense against such attacks is not recognized under this treaty. To support his argument, Schmitt cited the Vienna Convention on the Law of Treaties which sets the interpretive principle that treaties are to be interpreted in accordance with, "the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and scope" (p. 13). For this reason, he argued that the word "armed force" as cited in the U.N. Charter does not apply to cyber attacks. Schmitt further argued that had the U.N. intended other forms of attack to fit the scope of the charter then the drafters would have included it in the language of the charter.

2. With regard to applying a cyber deterrence strategy similar to the nuclear deterrence strategy during the Cold War at least one scholar (e.g. Solomon, 2011) believed that cyber deterrence was ineffective because these attacks are mostly conducted covertly. Solomon argued that unlike nuclear and conventional warfare, actors in a cyber attack can hide their activities thereby avoiding a deterrence trigger. In other words, deterrence was effective during the Cold War because it was an overt activity—nukes cannot be launched covertly. However, in cyber warfare, Solomon argued, "the attacker may go to great lengths to conceal that an event was caused by a cyber attack, particularly if the attack was designed to covertly support diplomatic, economic, or military initiatives in other areas" (p. 12).

CONCLUSION

It is evident from the literature that despite the counterarguments to treaties and deterrence postures, against cyber attacks, they are the best courses of action to take thus far. In 1991, a landmark national research council concluded that, "We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services…tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (Sterner, 2011, p. 63). Not surprisingly, 20 years later these revelations have come to manifest themselves. Therefore, the writer believes that given the interconnectedness of cyberspace and the increasing threats to our critical infrastructures and key resources it is necessary to draft a cosmopolitan treaty of non-aggression via cyber attacks. Beidleman (2009) emphasized this point very eloquently, "cyber attacks against the infrastructure or economies of other states can have severe, cascading effects on the U.S" (p. 19). The writer proposes that such a treaty follow in the language of the Kellogg-Briand Pact of 1928, also known as the Pact of Paris, to outlaw war. In this cyber treaty, state sponsored cyber attacks against critical infrastructures or key resources of any sovereign nation are considered armed attacks and therefore illegal, and subject to severe retaliation either unilaterally or bilaterally. The form of retaliation could be either kinetic or non-kinetic (Figure 1) as long as it met the Jus in bello rule of war (i.e. an eye for eye):

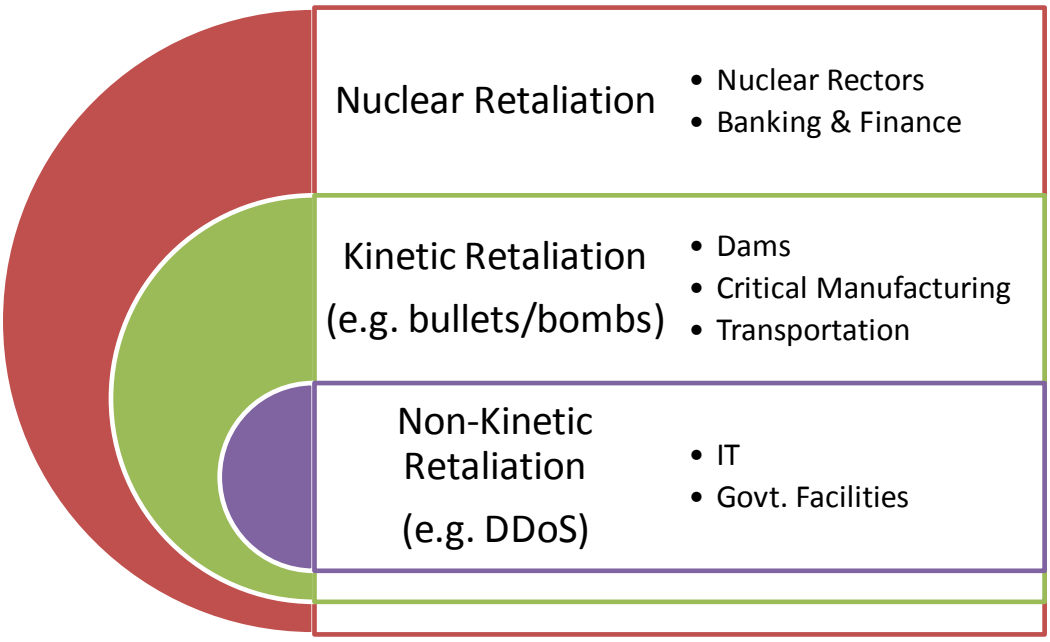

Figure 1. Suggested levels of response against breach of cyber treaty

In conclusion, the writer is convinced that such a treaty, as the one proposed here, serves as the best strategy to date because like the nuclear deterrence posture of the Cold War it carries a huge psychological impact—fear of annihilation.

BIBLIOGRAPHY

Beidleman, S.W. (2009). Defining and deterring cyber war. *U.S. Army War College*, 1-36. Retrieved from http://www.hsdl.org

Graham, D. E. (2010). Cyber threats and the law of war. *Journal of National Security Law & Policy, 4*(87), 87-102. Retrieved from http://jnslp.com

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012).

The law of cyber-attack. *Yale University*, 1-76. Retrieved from http://www.law.yale.edu

Hoskins, A., Liu, Y., & Relkuntwar, A. (2005). Counter-attacks for cybersecurity threats.

University of Washington, Computer Science and Engineering. Retrieved from http://www.cs.washington.edu

Jensen, E. T. (2002). Computer attacks on critical national infrastructure: A use of force invoking the right of self-defense. *Stanford Journal of International Law, 38*, 207-240. Retrieved from http://papers.ssrn.com

Libicki, M. C. (2009). Cyber deterrence and cyber war. *The RAND Corporation*, 1-175. Retrieved from http://www.rand.org

Mudrinich, E. M. (2012). The Department of Defense strategy for operating in cyberspace and the attribution problem. *Air Force Law Review, 68*, 168-205. Retrieved from http://www.afjag.af.mil

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Institute for Information Technology*, 1-41. Retrieved from http://www.dtic.mil/dtic

Schiller Institute (n.d.). *The Treaty of Westphalia, 1648*. Retrieved from http://www.schillerinstitute.org

Solomon, J. (2011). Cyberdeterrence between nation-states: Plausible strategy or a pipe dream? *Strategic Studies Quarterly*, 1-25. Retrieved from http://www.au.af.mil/au

Sterner, E. (2011). Retaliatory deterrence in cyberspace. *Strategic Studies Quarterly*, 62-79. Retrieved from http://www.au.af.mil/au

United Nations (n.d.). *Charter of the United Nations*. Retrieved from http://www.un.orgU.S. Department of State (n.d.). *The Kellogg-Briand Pact, 1928*. Retrieved from http://history.state.gov

PART VII: LEGAL

Legal Authorities and Ramifications of Offensive Cyber Operations
Major John E. Henley, U.S. Air Force (USAFWC/A8Z)

ABSTRACT

Due to the relatively recent introduction of offensive cyber operations onto the world stage and the lack of definitive international customs or law related to their conduct, the legal ramifications and impact of their use is murky at best. While there is relative agreement amongst the international community about what constitutes "use of force" and an "armed attack" in regards to kinetic operations, non-kinetic operations, to include, cyber, have not been adequately addressed. This lack of international consensus combined with often unrealistic concerns of collateral damage has led the United States (U.S.) to require the legal authorities for offensive cyber operations be held at the highest level of the U.S. Government, making it difficult to effectively utilize these capabilities. In order to effectively utilize its offensive cyber capabilities while simultaneously ensuring the ability to appropriately defend against and respond to enemy offensive cyber operations, the U.S. should lead the international community in codifying what constitutes a cyber attack and the acceptable responses nation states should be allowed to make.

DESCRIPTION OF ISSUE

1. While the pace of technological innovation, as well as the skills associated with such innovation, has ensured that the cyberspace domain and its associated hardware and software has advanced in line with Moore's Law, the laws of the international community have not kept up with these advances. With the singular exception of the Convention on Cybercrime, an international treaty originally signed in 2001 and currently ratified by 37 countries to include the U.S., no international law or customs exist to explicitly govern activities within computer networks or the cyberspace domain.[1] And while this treaty covers cybercrime and nation states' responsibilities to prevent it, of specific interest to the U.S. military is the complete lack of international laws or legal decisions regarding the use of offensive cyber operations as an element of military force. This dearth of cyber specific legal rulings has led individual countries to attempt to interpret existing international law, treaties, and customs as they relate to cyber operations.

2. The Law of Armed Conflict (LOAC) is the most widely accepted international standard relating to war and offensive military operations and is derived from international laws as established in the Charter of the United Nations (UN).[2] The LOAC specifically acknowledges two primary questions related to armed conflict; when is it legal for nations to utilize force against each other, *jus ad bellum*, and what is the appropriate behavior of nations and combatants engaged in armed conflict, *jus in bello*.[3] While the body of law known as *jus in* bello is important to the conduct of combatants, to include cyber combatants, once they are engaged in armed conflict, a discussion on these rules is beyond the scope of this paper. Under the body of law known as *jus ad bellum*, the UN prohibits "the threat or use of force against…any state," under Article 2.4 of the UN Charter.[4] However, no definition of force in this context is provided within the UN Charter, nor has one since been defined in either treaties or any other international agreements; instead, nations rely on historical precedents to determine what constitutes a "threat or use of force."[5] Also falling under the rubric of *jus ad bellum*, Article 51 of the UN Charter asserts a nation state's right of self-defense if an "armed attack occurs," but again does not define what an "armed attack" is.[6] While the phrases "use of force" and "armed attack" are generally

understood in relation to conventional, kinetic attacks via past precedents and state declarations, no direct precedents exist to aid in discussion of offensive cyber operations.[7]

3. These ambiguities in terminology and lack of precedent in international law provide a difficult obstacle to overcome before nation states can be held accountable for conducting offensive cyber operations against others. While various models have been developed for the purpose of applying "[Jean] Pictet's use of force criteria – scope, duration, and intensity" to offensive cyber operations, the fact remains that the international community has yet to recognize a common standard or custom in dealing with these means of attack.[8] This lack of international law is further compounded by the inherently difficult nature of attributing offensive cyber operations back to their source.[9] While the simple identification of an attacking IP address may be sufficient for the application of passive cyber defensive actions, identifying the actual source of an attack is severely hampered by the ability of attackers to utilize the very nature of the Internet itself as its "design…lends itself to anonymity."[10] Without the ability to attribute cyber attacks against their systems, nation states are left with the inability to plead their case in front of the international community. This in turn ensures that decisions on how to deal with cyber attacks will not be forthcoming as the international community is unlikely to weigh in on attacks where attribution cannot be guaranteed. This apparent legal freedom potentially allows nation states, as well as non-state actors, to operate with near impunity within the cyberspace domain while ensuring there is no way to punish or effectively issue a demarche against a country for malicious cyber activity.

4. This lack of international laws or guidelines further inhibits U.S. offensive cyber operations, as there are no clear cut guidelines as to when these operations can be used outside of a state of war or armed conflict. As a result, the authority to execute offensive cyber operations against another nation state are often held at the highest levels of the chain of command; in some cases only the President can authorize these offensive cyber operations, often delaying or denying the ability to effectively execute in the rapidly changing cyber battlespace.[11]

RECOMMENDATION

1. In order to ensure the U.S.' freedom of movement within the cyberspace domain, as well as ensure that strategic, operational, and tactical decisions can be made with a basis in international law, the U.S. should make a concerted effort to lead the international community in the development of international law related to offensive cyber operations. As discussed previously in this paper, the LOAC is no longer sufficiently able to govern modern warfare and the emerging technical capabilities of the cyberspace domain. However, the guiding principles that underline the LOAC can and should be referenced when developing laws to govern the use of offensive cyber operations in peace and war.

2. Before any discussion of potential recommendations on how offensive cyber operations should be legally governed can take place, it is first important to define those operations. For the purposes of this paper, we will use the definition developed by Herbert Lin; "military operations and activities in cyberspace for cyber attack against and (or) cyber exploitation of adversary information systems and networks."[12] Two means of offensive cyber operations are delineated in this definition; cyber attack, "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these

systems or networks," and cyber exploitation, "the use of cyber offensive actions…usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks."[13] The distinction between these two types of operations is significant, as the way the LOAC views these types of operations is quite different. Cyber exploitation is recognized by many nation states, to include the U.S., as simply another means to conduct espionage which is considered permissible under the LOAC and are not considered illegal under international law.[14] Problems arise, however, due to the fact that the tools and techniques utilized in the conduct of cyber exploitation are similar, if not the same, as those used in a cyber attack with the primary difference being the intent of the operator.[15] These problems notwithstanding, the precedent for considering cyber exploitation as espionage allows for the aperture of new international law to focus on cyber attack operations.

3. The primary purpose of any new laws governing cyber attack should be to reconcile them with already existing laws, like the LOAC. The most important question that must be asked within the context of the LOAC is whether a cyber attack can or should ever be considered a "use of force" under Article 2.4 of the UN Charter, or more importantly an "armed attack" under Article 51. Much thought has been put into this integration of cyber warfare with the LOAC and it would be detrimental to overlook the work that has already been accomplished. Among the many models and recommendations that have been put forth throughout the community, an effects-based approach seems the most logical and consistent with U.S. policy and its approach to warfare. While other models focus on whether a cyber attack causes damage pursuant with the damage that might be caused by a kinetic attack, this effects-based model is more concerned with the "overall effect of the cyber attack on the victim state."[16] Thus this model allows for cyber attacks that have a significant impact on the victim state but could not have been replicated by a conventional kinetic strike.[17] Today many nation states have much of their government and civilian information housed solely within the cyberspace domain, and such an attack could prove as costly and devastating as a kinetic strike. Imagine a case where an aggressor uses a cyber attack against its enemy and destroys or erases all of the databases associated with their passport and immigration systems. The financial cost, not to mention the potential security risks, associated with the loss of all of the data would be substantial. By clarifying what cyber attacks constitute a "use of force" and "armed attack" within international law, the U.S. and its allies would have the opportunity to seek international sanctions against those actors whose cyber attacks could be attributed to them.

4. By leading the development of international law, the U.S. would put itself in a position to clearly steer the legal issues related to cyber attack in a direction that supports U.S. national security and interests. Additionally, by developing a clear delineation of when a cyber attack reaches the threshold of "use of force" or "armed attack", as well as legal parameters outlining acceptable response options when other nation states conduct cyber attacks against the U.S., it would enable the authorities to execute some offensive cyber operations and allow them to be delegated to a lower operational level when certain triggers have been met. Finally, if international laws are in place, nation states would be obliged to provide support to cyber attack attribution when an attacker's IP address has been traced back to their state.

COUNTERARGUMENT

1. The ambiguities present within international law in regards to cyber operations could prove beneficial to the U.S. and its allies. Without a clear definition of what constitutes a cyber attack,

and when a cyber attack reaches the level of "use of force" or "armed attack," nation states are allowed to operate within a large grey area with few legal ramifications as a result of their actions. As one of the most technologically advanced countries in the world, it stands to reason that the U.S. would have significant offensive cyber operations capabilities whose uses could benefit from this ambiguity.

2. In addition, while the U.S. typically feels compelled to comply with international law, many nation states at odds with the U.S. do not. By codifying laws dealing with cyber attacks, the U.S. may simply be limiting its ability to conduct offensive cyber operations and react to the cyber aggression of others, while its enemies continue to operate with impunity in clear violation of international law. Since attribution is such a difficult problem within cyberspace, it becomes very difficult to identify the source of cyber attacks to a level of fidelity that would be required to accuse or prosecute a cyber aggressor in the international community. Thus the U.S. could be put in a situation where another nation state or non-state actor is conducting cyber attacks against it, but has no way to retaliate or seek international condemnation because clear attribution cannot be identified.

CONCLUSION

The development of the computer network, the integration of worldwide networks into the Internet, and the global reliance on information systems to process and store information may constitute the single most innovative leap in technology in human history. Since the first time man took up arms against another, warfare and conflict has continued to evolve. However the intersection of technology and the cyberspace domain with warfare has created a fundamental change in what is now considered warfare. While weapons have continued to improve, and man has developed means to operate in physical domains never thought possible before, at its fundamental level warfare has been about killing people and destroying things for a national purpose. And at their most fundamental level, this is what the laws, customs and treaties developed by the international community have been designed to govern. But the advent of cyber technology and the development of the cyberspace domain have significantly altered what constitutes a target and how destructive non-kinetic attacks can be. Without codified international laws developed to govern offensive cyber operations, nation states will be free to conduct operations within cyberspace without fear of reprisal from the international community. As one of the most prolific developers and consumers of information within the cyberspace domain, as well as being heavily reliant on cyber systems much of its national infrastructure, it behooves the U.S. to take the lead amongst the international community to develop these laws, and not wait for a "cyber Pearl Harbor."

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Council of Europe, "Convention Committee on Cybercrime (T-CY)," http://www.coe.int/t/dghl/standardsetting/t-cy/Default_en.asp
2. Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Secuirty Law and Policy,* Vol. 4 (2010): 71.
3. Ibid.

4. United Nations, *Charter of the United Nations and Statue of the International Court of Justice*. (1945).
5. David E. Graham, "Cyber Threats and the Law of War.," *Journal of National Security Law and Policy*, Vol. 4 (2010): 90.
6. United Nations, *Charter of the United Nations*.
7. Graham, "Cyber Threats and the Law of War," 90.
8. Ibid., 91.
9. Ibid., 92.
10. Air Force Directive Document 3-12 (2010), *Cyberspace Operations*, 10.
11. Ibid., 11.
12. Lin, "Offensive Cyber Operations and the Use of Force," 64.
13. National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, ed. William A. Owens, Kenneth W. Dam, and Herbert S. Lin (Washington, DC: The National Academies Press, 2009), 1, 11.
14. Wortham, Anna, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force," *Federal Communication Law Journal*, Vol. 64 (2011): 652.
15. National Research Council, *Use of Cyberattack Capabilities*, 22.
16. Graham, "Cyber Threats and the Law of War," 91.
17. Ibid.

BIBLIOGRAPHY

Air Force Directive Document 3-12 (2010). *Cyberspace Operations*. Council of Europe. "Convention Committee on Cybercrime (T-CY)." http://www.coe.int/t/dghl/standardsetting/t-cy/Default_en.asp

Graham, David E. "Cyber Threats and the Law of War." *Journal of National Security Law and Policy*, Vol. 4 (2010): 87-102.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law and Policy*, Vol. 4 (2010): 63-86.

National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin. Washington, DC: The National Academies Press, 2009.

United Nations. *Charter of the United Nations and Statue of the International Court of Justice*. (1945).

Wortham, Anna. "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force." *Federal Communication Law Journal*, Vol. 64 (2011): 643-660.

When is Cyber Attack Legal & Justified?
Major Samuel D. Brown, U.S. Air Force (302 ALW)

ABSTRACT

We know how to conduct war. We have waded through various fields of conflict on land, sea, air, and space.[1] Taking the offensive to the enemy in battle is not new to us and whether we in the past have used a trebuchet, a long bow, a cruise missile or a pulse of electromagnetic energy, we have adopted a balanced approach of defensive and offensive operations to achieve our national objectives. The sophistication of the tools and our methods of their use have evolved. And now our doctrine and rules of engagement must adapt and become formalized so that we can effectively accomplish our responsibilities for national defense. This doctrine must now formally include new capabilities in the domains of cyber defense and attack. In fact these new weapons must be used holistically and integrated into future military endeavors. The effective use of offensive cyber tools is hindered by a lack of specific legal and doctrinal frameworks to align their use. This paper will outline the relevant frameworks that currently exist for cyber attack and discuss specific areas that must be strengthened, addressed or better understood to secure success in current and future cyber operations.

DESCRIPTION OF ISSUE

1. Our laws, doctrine, policy, and strategies are evolving. We live in a society with unprecedented access to inexpensive, globally interconnected computing systems. This new technological abundance has leveled the international "playing field" in many industries and has created a demand for continued advancement as society enjoys a flattened new world rich with information and access.[2] This new reality has created a security paradox where our demand for advancement strains our ability to protect those same systems, structures and the information shared between them. As our technology outpaces our ability to defend it, our enemies have demonstrated both the will and wherewithal to attack our national commercial and defense infrastructure as if they were one in the same. While their motives may not always be clear, their attacks are persistent and pervasive. As their capabilities continue to mature it is becoming an increasing imperative to align the authority, frameworks, and resources to support and protect our national interests. Additionally, we have proven over time the Clausewitz theory about the superiority of the defense over the offense but this cannot be at the expense of or in place of a strong offensive posture or capability.[3]

2. Legal parameters that govern this cyberspace internationally are weak. Ironically this reality allows far more latitude for current and future operations. Currently the only alignment with international language in policy documents or statements comes from *Article 51* of the United Nations charter which states that "Nothing…shall impair the inherent right of self-defense if an armed attack occurs against a Member of the United Nations." While the term "armed" attack is problematic in the context of cyber operations, our right to self-defense characterizes our current position as we stand before the international community. Article two becomes relevant in the event that cyber offensive operations contribute to what might be considered to be "a use of force against territorial integrity or political independence." This would be prohibited if it could not be established that it was used under the *Article 51* provision as an act of self- defense. In 2001, an international treaty was established through the *Convention on Cybercrime* to address criminal policy and Internet crime and was designed to both harmonize nations' domestic cybercrime laws and improve domestic investigation and

prosecution.[4] This is a relevant body of international consensus if we consider the blurred effect of current attack methodologies which are not required to discriminate between national defense systems or private commercial systems.

3. U.S. military doctrine must not only create the conditions to ensure successful offensive cyber operations, it should actively promote them and allow for the adaptation of strategy and tactics in this fast paced, constantly evolving domain. Clausewitz established that we enter into war as an extension of policy and to achieve political objectives.[5] While this largely remains the case, what continues to evolve and change are the means to achieve those ends. The tools, tactics, techniques, and protocols used to achieve these objectives are often subtle and stealthy and less kinetic and overt. For the purpose of this paper, it is critical that we understand the definition and purpose of military doctrine. Its most concise definition comes from researchers at Air University who simply state that "Military Doctrine is what we believe about the best way to conduct military affairs." This may not immediately resonate as a powerful definition, but the word "believe" suggests that a thorough examination and interpretation of all available evidence did occur before establishing direction. It also allows for adjustments to interpretation when new evidence is introduced. There are no strict laws within military doctrine; they are interpretations of what we know or believe. The word "best" suggests a stratification or rank method of prioritization.[6] Our military doctrine and posture must balance a strong defensive and offensive capability. Ultimately, offensive cyber mechanisms will be a natural extension of any military operation within all of the relevant domains of the battlespace. Theories abound and the possibilities exist for kinetic operations in this arena. Within the past several years we have come the closest to seeing the potential for cyber attacks, and theory allows us to imagine how cyber operations might cross the kinetic threshold of destruction via physical attack (it should be noted here that the 1982 Siberian pipeline explosion could also be an example of software manipulated to cause a catastrophic failure. However, the facts regarding the actual event and loss of life claims are unsubstantiated and controversial).

4. We lack a universally-acceptable vocabulary and common conceptual framework. This hinders the development of policy and legal framework development because leaders are unable to adapt them to their planning models or are unaware of their overall capabilities. The more familiar senior leaders are with the capabilities that cyber attack can provide to the battlespace, the more likely they will be to integrate their use. Gen C. Robert Kehler, Commander of United States Strategic Command, described the domains of space and cyberspace as becoming "increasingly intertwined with the traditional domains of land, sea, and air."[7] There continues to be wide disagreement even among the most senior leaders as to whether cyberspace is its own domain or whether it transcends the traditional domains. This simple struggle with definition characterizes a broader struggle to establish the terms, definitions, and semantics of cyberspace.

5. There is still a need to address several cyberspace imperatives. It is reported that a *Presidential Policy Directive* (PPD-20) has been issued that establishes policy for how the Defense Department addresses cyber threats and among other things, collaborates with civilian agencies.[8] Rules of engagement are typically classified and not for general release so this direction is not public knowledge. It is a promising move that hopefully provides more specific direction in order to bridge the gap between our current policies and the practices needed to allow us to protect and defend our national interests through the use of our total force capabilities to include offensive measures. It is anticipated that this direction allows the military to work

more closely with civilian agencies. State sponsored attacks against all national infrastructures have blurred lines between what constitutes a threat requiring a national defense response or a law enforcement response. Our national policy has not yet adapted in an acceptable way to protect and support our new dependence on technology. In fact, it should be noted that most of our national infrastructure, including the Internet itself, is currently managed commercially, creating tension between Posse Comitatus and the Title authority from the U.S. code for military, intelligence, National Guard, and law enforcement.

RECOMMENDATION

1. Our priority and long term goal should be to establish strategic superiority in cyberspace. This must include national priorities to train and equip in order to maintain depth and breadth of offensive and defensive cyber frameworks and capabilities. Our policies must be adaptable in order to address threats which are not yet known. They must also dictate authority and thresholds to establish priority and order of response in order to act quickly, decisively, and effectively. Additionally, our national infrastructure should leverage expertise, regardless of which sector it comes from. The public, private, government, and defense organizations should leverage capabilities and strengths and incorporate international entities where appropriate.

2. We must establish similar agreements and rules of engagement with our allies. Deterrence protected the world during the cold war but has to date been an ineffective strategy in the cyber realm. While our doctrine, policy, and legal systems are maturing to support a strong national posture within cyberspace, clarity is still needed to provide clear lines of responsibility abroad. In addition, the proper balance between freedom and what is required to defend our national infrastructure cannot be ignored and performing offensive acts against other individuals, organizations, nation-states or their resources should be a more common response in order for it to be perceived as a viable threat. This is a new type of war and requires new aggressive yet responsible rules.

3. In the short term we should build and train to an acceptable level of cyber expertise and maintain those core competencies within our forces. We must develop, mature, and harden the appropriate tools, tactics, techniques, and protocols to effectively support offensive operations. Cyber defense must include an offensive component that may be wielded kinetically and should push existing theory within non-kinetic attack. We must establish responsible yet real retribution mechanisms to dissuade nation state attacks. To that end, we must consider whether or not to adjust parameters within our definition for what constitutes “an act of war.” Traditionally, we have used death, damage or destruction to determine what would be a use-of-force and merit retaliation.

4. Legislators must integrate, adapt or change proposed legislation within the existing framework and initiatives, such as DOD’s *Strategy for Operating in Cyberspace*, the White House’s *National Security Strategy* and *International Strategy for Cyberspace*, and DOD’s *Quadrennial Defense Review*. Our lexicons, strategic documents, and frameworks must be established quickly using common terms and then adjusted as needed based upon new knowledge and information. Our military priorities and posture are extensions of our national political objectives and priorities. The President has clearly stated that the United States “will respond to hostile acts in cyberspace as we would to any other threat to our country.” He clarified that we would exhaust all options prior to using force whenever possible and would

"carefully weigh the costs and risks of action against the costs of inaction." He went on to direct that the DOD would ensure that the "U.S. military continues to have all necessary capabilities in cyberspace to defend the United States and its interests, as it does across all domains."[9] This declaration allows for more latitude and permission to address and counter cyber threats and the potential use of offensive methods.

5. General Kehler testified March 2012 to the Armed Services Committee and stated that "We need to adjust the framework that we use for military command decisions in cyberspace." He stated that most of the current capabilities within our fleets, air wings, and brigades lie in the areas of how to operate and defend. He asserted that our "offensive capability primarily lies in the exploitation capabilities of the NSA (National Security Agency) and others." But he contended that we are developing offensive capabilities as part of a deliberate growth plan. One of his clear messages to that committee was that we need to collaborate within industry to leverage expertise in the realm of detection and defense. An existing footprint of expertise exists in other national sectors and similar infrastructure and equipment exists nationally as we all generally use commercial-off-the-shelf products to build, support, and maintain our systems. Leveraging expertise at least at the Network and systems defense level would allow us to better align resources and adjust priorities in order to focus on and better mature offensive capabilities. Ultimately PPD 20 must address the thresholds and direction for when we can exploit, disrupt or destroy in the realm of cyberspace. To be effective, it should also articulate who has the authority to use offensive cyber measures and how or when it is justified. Eventually we will need to relook at longstanding methodologies for determining the impact of military operations. Areas such as proportionality and limited effect have given us kinetic frameworks for the battlespace. We must establish new or adapt existing frameworks to describe cyber effects in the same manner. Regarding state sponsored attacks, relevant questions remain regarding what constitutes an act of war. "Plenty of (cyber) incidents of espionage, harassment, theft and even targeted attacks have been widely publicized, but so far, none have escalated into armed conflict.[10]

COUNTERARGUMENT

The main caution is that if we move too quickly into the development of doctrine and law for offensive cyber operations it could hinder us and possibly restrict our ability to defend our national interests in the Cyber Domain. This would require broader study to analyze current policy in an attempt to harmonize existing legal frameworks to suit our needs. The rule of law is crucial but speed is not really required because this is a new international domain and it's extremely challenging to assign attribution in order to potentially establish offensive plans to attack. Additionally, any cyber attack in such a fragile untested domain against an enemy who may only be a proxy for the real enemy could cause more harm than addressing cyber doctrine in a more deliberate and thorough manner. If we had a clearer common understanding of the issues we would be able to debate them more thoroughly. Finally, our traditional enemies and our unconventional enemies are not bound by law or strict doctrine. In this regard it could prove to be a disadvantage to establish formality and parameters too quickly. While the current ambiguity is impeding policy development, it could provide greater flexibility to leaders in the cyber domain. Another potential issue with talking too boldly about American plans and publicizing this debate is that it could add more incentive to a global computer arms race.

CONCLUSION

The Internet began as a benign and interesting research project[11] whose intent was to create redundancy with limited application to our national security. Today it has become critical to our national infrastructure. Our ability to defend and wage war in a digital arena will be a priority in all future military planning and strategy. Nations previously unable to pose a real threat due to the lack of resources or a modern traditional military can now engage in a new battlespace, with relatively equal footing and sponsor attacks to destabilize, extort or cripple adversaries with minimal expense or exposure. Every country, military apparatus and commercial entity is connected to this superhighway of access to one another through porous boundaries and varied mechanisms of protection. As countries aggressively pursue capabilities to gather advantage and wage battle in this new Cyber Domain, we must establish common language in order to establish clear doctrine, legal authority, and acceptable thresholds of response that include offensive countermeasures in order to defend our national interests. A comprehensive offensive threat must exist in air, sea, land, space, and cyberspace and must be made up of kinetic and non-kinetic offensive capabilities to ensure that we can effectively achieve superiority in the domain of our choosing.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Thomas C. Wingfield, "*Legal aspects of offensive information operations in space*," *USAF Acad. J. Legal Stud*ies 9 (1998): 8.
2. Thomas L. Friedman, *The World Is Flat: a Brief History of the Twenty-First Century*, Rev. pbk. ed. (New York, NY: Picador, 2007), 7.
3. W.B. Gallie, *Philosophers of Peace and War: Kant, Clausewitz, Marx, Engels and Tolstoy* (Cambridge: Cambridge University Press, 1978), 49.
4. *Convention on Cybercrime*, Budapest, 23 November 2001, www.conventions.coe.int/Treaty/en/Treaties/HTML/185.htm
5. Carl Von Clausewitz, Carl, and Colonel JJ Graham, *On war*, (Digireads. Com, 2008), page 34
6. Dennis M. Dreww and Donald M. Snow, *Making strategy: An Introduction to National Security Processes and Problems*, (Air Univ MAXWELL AFB AL, 1988), pp. 163
7. Gen C. Robert Kehler, Commander, USSTRATCOM, 5/5/2011, *National Space Symposium Keynote*, http://www.stratcom.mil/quotes/2011/16
8. Bloomberg, *Obama Issues Presidential Directive on U.S. Cyber Operations*, Nov 14, 2012, http://www.bloomberg.com/news/2012-11-14/obama-issues-presidential-directive-on-u-s-cyber-operations.html
9. President Barack H. Obama, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf
10. General Robert Kehler, the Commander of the U.S. Strategic Command testifying to the U.S. Senate Committee on Armed Services, Washington D.C. "*Hearing to receive testimony on U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for FY2013*" March 2012, http://www.armed-services.senate.gov/Transcripts/2012/03%20March/12-19%20-%203-27-12.pdf

11. Gary Chapman, "*National Security and the Internet*," Paper presented at the annual convention of the Internet Society, Geneva, Switzerland in July, 1998, http://www.utexas.edu/lbj/21cp/isoc.htm

BIBLIOGRAPHY

Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, Mass.: Syngress, 2011

Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: The Penguin Press, 2011

Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, Issue 1, (2012)

Cyber Attack Policy and Legality

Major Randall R. Pouliot, U.S. Air Force (HQ AETC)

ABSTRACT

The United States (US), and specifically the Department of Defense (DOD), is under relentless attack from various actors (e.g. nation-state, terrorists, and criminal networks) around the globe. These attacks could be seen as requiring a cyber response, however the cyber domain differs vastly from the physical domains of land, sea, air, and space in which international law applies. This difference requires explicit rules and guidance to provide top-cover to cyber warriors in executing cyber attacks so as to minimize its risk, demonstrate morality all the while without hindering U.S. operations. This paper will discuss the current international laws as they relate to cyber attack, how the laws may be seen as crippling to the U.S.' potential use of cyber attack as an extension of our military instrument of power and what can be done to update current US military doctrine to ensure freedom of action at the time and place of our choosing in order to achieve national objectives.

DESCRIPTION OF ISSUE

1. According to international law as imposed by the Geneva and Hague Conventions, United Nations (UN) Charter, and the Cybercrime Convention, cyber attacks are considered an armed attack.[1] And the U.S. is under constant cyber attack according to outgoing Secretary of Defense Leon Panetta "[w]e are literally the target of thousands of cyber attacks every day"[2] and he went on to indicate that cyber attackers have the capability to:

> Strike at government, strike at the defense department, and our intelligence agencies. Cyber is now at a point where the technology is there to cripple a country, to take down our power grid systems, to take down our government systems, take down our financial systems, and literally paralyze the country."[3]

Recently the US Department of Homeland Security (DHS) confirmed such an attack "announc[ing] that an American power station, which it did not name, was crippled for weeks by cyber attacks."[4] What options does the U.S. have when confronted with these attacks in this often misunderstood, but highly contested domain of cyber?

In order to better understand U.S. cyber response it's essential to first comprehend international law, specifically the law of armed conflict (LOAC). It is LOAC that addresses when is it legal to use force against another nation, which is known as *jus ad bellum*, and when in conflict what are the rules of combat, which is known as *jus in bello*. Firstly *jus ad bellum* is administered by the UN under several charters, with Article 51 being more specific: "the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[5]

In addition to self-defense, a nation is also allowed to defend itself in the case of an imminent attack, which is known as "anticipatory self-defense". Thus if the U.S. believed an attack were plausible against DOD systems, the U.S. could, under Article 51, defend itself. However a U.S. response would need to meet certain aspects in order to be considered lawful and most importantly morally correct in the court of public opinion. White House spokesman Jay Carney

recently was quoted as saying "[w]e conduct…strikes because they are necessary to mitigate ongoing actual threats, to stop plots, to prevent future attacks and, again, save American lives."[6] Once a cyber attack was to take place regardless of being preemptive or not, *jus in bello* applies with the following limitations of military: necessity, proportionality, perfidy, distinction, neutrality, and discrimination. As long as these constraints are properly applied regardless of the type of attack, in this case cyber, the international laws would be considered duly met thus ensuring legality of attack. Thus, per international law, a cyber attack is considered an armed attack and must be executed in accordance with LOAC.

Given cyber's unique characteristics this domain requires explicit rules especially given that:

> Cyberweapons are newer…have certain characteristics not shared with kinetic weapons, which implies that fewer precedents and analyses are available and that the application of LOAC principles may not be as straightforward as they are when kinetic weapons are involved.[7]

2. Cyber is a unique, man-made domain, which makes targeting challenging. In the other physically limited domains where, for example, a ship can only reside in one location, targeting is more explicit. Conversely in the cyber domain a target may seem to reside in one specific location, however it may prove difficult to ascertain it's absolute physical location and most importantly the relationship of the cyber target with other interconnected, but untargeted systems. This aspect of targeting is critical to LOAC's limitations in that "[t]he cardinal legal and ethical principles of distinction and proportionality require technical data that will inform decision makers as to who might be affected by a particular technique, and to what extent."[8]

3. Cyber attack legalities prove difficult depending on the timing, actor, and physical location. The timing of a cyber attack is critical from a response point of view in that if a cyber attack were executed either preemptively or as part of ongoing operations. As mentioned above, Article 51 may provide enough top cover. However, public opinion may vary as seen in the U.S./Israel Stuxnet attack on Iran. The cyber attack target's perpetrator, known as the actor (i.e. nation-state, terrorist, criminal network) also divides the legalities of a cyber attack because although nation-states are seen as the traditional target, "LOAC and the UN Charter are largely silent on how to address conflict involving non-state actors, even though non-state actors (in particular, terrorist groups) are playing larger roles in the security environment today."[9] Carving out the legal aspects of a cyber attack on these varying actors may prove necessary to ensure attacks are legally and morally accurate.

Lastly, the intermediate locations to reach a cyber target and the end-point location of a cyber target are also problematic. This "[p]hysical location is important because of the legal jurisdictional issue—depending on the physical (national) location of the hardware, different laws regarding the punitive criminality of its behavior and the legality of damaging it may apply."[10] Considering the eventual end-point, targeted attacks will usually be launched from an intermediate location (not in the U.S.), meaning the end-point is usually targeted from a foreign location vice directly from US soil. Given the legal aspects of cyber attacks and the moral perspective through which the cyber effects are viewed, it's important to advance the public understanding of cyber attacks and also to provide cyber warriors a more detailed toolset to accomplish the cyber deterrence mission.

RECOMMENDATION

1. Joint Publication (JP) 3-60, *Joint Targeting*, should specifically include cyber detailed targeting language. Targeting in joint doctrine is defined as "the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.[11] Although targeting may seem simple, it is extremely complex within cyber as considered when attempting to ascertain a cyber target's location, perpetrator/actor and timing. The cyber warrior would be hard pressed to find cyber targeting in other Joint Publications, although it is somewhat discussed in JP 3-13, *Information Operations*, it may be best to revert to service doctrine, specifically within "AFDD 3-12 [which] discusses many issues useful in cyber targeting, such as technical relationships in cyberspace infrastructure, information assurance, compressed decision cycles, and the anonymity and attribution challenge, it does not specifically address cyber targeting per se."12 Given the above it would best serve the cyber warrior if a JP did provide the granularity necessary for operating in the unique cyber domain.

Additionally, JP 3-60 does "[f]rom a legal perspective, [provide] adherence to the joint targeting cycle process…coupled with sound command judgment, virtually assures compliance with the laws of war."[13] This makes JP 3-60 a good starting point in further refining cyber targeting as utilized by military planners and cyber warriors alike. Overall cyber targeting refinements necessary in an updated JP 3-60 include an initial statement that:

> Fundamentals described in the publication apply to targeting in the newly recognized cyber domain. Such a statement would have the two-fold purpose of recognizing the importance and uniqueness of military operations in cyberspace and affirming the universality of the publication's combat-targeting principles."[14]

Further cyber updates to JP 3-60 should include the "complexity of the cyber domain", "differences between offensive and defensive cyber targeting", and "the concepts of an adversary's cyber center of gravity and a cyberspace joint operations area."[15]

2. Develop a cyber framework based on desired effects. As pointed out by New York Times' David Sanger and Thom Shanker "what constitutes reasonable and proportionate force in halting or retaliating against a cyberattack"[16] further demonstrates that targeting is difficult and requires specific direction and refinement to ensure a cyber attack is legal and moral. Major General (ret) Dunlap, currently the Executive Director of the Center on Law, Ethics, and National Security at Duke University Law School and a former U.S. Air Force judge advocate further states the necessity for a cyber framework by affirming that the "ability to model effects with dependable accuracy represents one of the most needed capabilities in the world of cyber operations."[17] He goes on to state that "[s]uch an ability would give decision makers—not to mention lawyers and ethicists—the kind of information that is essential for making reasoned judgments about employing a cyber methodology."[18] Within this effects-based framework, Major Steven Smart, the Chief of Strategic Communications, Office of the Judge Advocate General, Headquarters U.S. Air Force, Pentagon clarifies that it should specifically feature cyber operations in regards to "collateral damage estimation and battle damage assessment."[19]

3. Continue strategic messaging to promote U.S.' unilateral option of cyber action, specifically, cyber attack. Given the scale of attacks on US DOD networks, it's vital for the US to clarify its

position on cyber response actions by communicating the U.S.' the right to choose the type and time of said actions. This freedom should make it clear to not only nation-states but also lower level actors, that the U.S. is serious about protecting itself. A recent example of these clarified new U.S. policies showed:

> How the intelligence agencies can carry out searches of faraway computer networks for signs of potential attacks on the United States and, if the president approves, attack adversaries by injecting them with destructive code—even if there is no declared war."[20]

To further illuminate this position, a senior U.S. official stressed the fact that the U.S. had actually reserved its cyber armament use.[21] This view helps to promote the U.S. opinion that thus far the enemy has yet to see the full spectrum of US cyber operations. That same official went on to specify "[t]here are levels of cyber warfare that are far more aggressive than anything that has been used or recommended to be done."[22] The U.S. continues to hone its cyber capabilities in a U.S. classified document titled the "Comprehensive National Cybersecurity Initiative" (CNCI), "which was adopted as national policy in January 2008 as part of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)."[23] The CNCI is undergoing continuous updates and press releases from DHS and the White House alike in order to further the necessary strategic messaging to achieve cyber dominance.

COUNTERARGUMENT

1. Applying laws to cyber attack capabilities will burden U.S. and its security. Some would say no new precise authorities are required to carry out offensive cyber operations: "[l]awyers across the government have raised so many show stopping legal questions about cyber war that they've left our military unable to fight, or even plan for, a war in cyberspace."[24] Additionally, leadership within DOD has gone on the record to also discount the necessity for further cyber clarification. Gen Robert Kehler, USAF, U.S. Strategic Command commander and the current parent organization for U.S. Cyber Command "declared that he did 'not believe that we need new explicit authorities to conduct offensive operations of any kind'…he did "not think there is any issue about authority to conduct [cyber] operations."[25] Gen Dunlap went on to summarize that "warfighters apparently do not see an incompatibility with legal and ethical restraints and their ability to effectively plan for a war in cyberspace."[26]

2. Some also say that cyber attacks, like drone attacks, are unethical and cowardly. As stated recently by Pakistan's ambassador to Washington, Sherry Rehman: "U.S. drone strikes in Pakistan were a direct violation of our sovereignty, illegal, and counterproductive, producing more militants than they eliminate."[27] In testimony to Congress in 2009, a retired Australian Army lieutenant colonel, Dr. David Kilcullen, stated that leveraging weaponized UAVs against the enemy is considered gutless and pathetic by the enemy.[28] This same approach has been taken with U.S. cyber attacks as Gen Dunlap continues that "[q]uite obviously, one might rather easily apply his thesis to cyber operations and those who conduct them."[29]

3. Cyber attack in response to a threat is risky. This position was recently published in the New York Times, which Sanger and Shanker indicated "preemption always has been a disputed legal concept."[30] This was vividly demonstrated in President Bush's reason for invading Iraq in 2003, which was found to be erroneously constructed on flawed intelligence about Iraq's weapons of mass destruction.[31] Not having the full evidence necessary to persuade U.S. public opinion can prove detrimental to U.S. operations over the long run. Sanger and Shanker foster

this point by affirming that "[p]reemption in the context of cyber war raises a potentially bigger quandary, because a country hit by a pre-emptive cyber strike could easily claim that it was innocent, undermining the justification for the attack."[32] One senior DOD official indicated it's quite difficult to demonstrate to the public that an attack on lethal programming code is truly warranted.[33]

4. The threat of a "cyber Pearl Harbor" is over exaggerated. Although there seems to be vast amounts of evidence pointing to the need for boosting the U.S.' cyber capability, many view the justification for the build-up as over inflated and driven mainly by private sector profiteers seeking the billions in this potential arena.[34] Some go on to argue that the cyber threat in which the world should be most concerned with is actually the US. The Guardian's Glenn Greenwald recently indicated the U.S., not another nation, is itself the leading cyber-aggressor in the world and acts as such in order to bolster its capability to annihilate other nations and actors via cyber attacks.[35]

CONCLUSION

Although the counterarguments may seem to diminish the potential for U.S. cyber attack as a means of achieving national objectives, the recommendations made will help to provide the U.S. the necessary flexibility and refinement to further build out this vital offensive capability. Although refining cyber attack targeting and legalities could be seen as unnecessary or even burdensome, doing so could provide clearer guidance for the cyber warrior while continuing to articulate to would-be attackers that the U.S. takes cyber attacks seriously and will respond within U.S. and international law.

According to U.S. Cyber Command, they estimate U.S. companies are losing $250 billion in intellectual property every year[36] and it becomes rapidly apparent it's not just about an offensive military capability in its purest sense, it's about deterring further attacks on the U.S. be it either the DOD or our homeland's critical infrastructure. By developing and refining our cyber attack capability through redefined doctrine and framework coupled with the necessary strategic messaging to deter future attacks the US can ensure the legal and moral high ground is maintained all the while refuting the counterarguments that exist today.

REFERENCES

NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. National Research Council (NRC), "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", p. 241
2. CBS News, "Pentagon expands cyber defense amid daily attacks"
3. Ibid.
4. Sanger and Shanker, "Broad Powers Seen for Obama in Cyberstrikes", New York Times
5. NRC, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", p. 243
6. Brisbane Times, "Killing of Americans by Drones is Lawful"
7. NRC, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", p.253
8. Dunlap, "Some Reflections on the Intersection of Law and Ethics in Cyber War", p.25

9. NRC, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, p. 251
10. NRC, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, p.145
11. Smart, “Joint Targeting in Cyberspace”, p. 66
12. Ibid., p. 69
13. Ibid., p. 70
14. Ibid., p. 72
15. Ibid.
16. Sanger and Shanker, “Broad Powers Seen for Obama in Cyberstrikes”, New York Times
17. Dunlap, “Some Reflections on the Intersection of Law and Ethics in Cyber War”, p. 25
18. Ibid.
19. Smart, “Joint Targeting in Cyberspace”, p. 71
20. Sanger and Shanker, “Broad Powers Seen for Obama in Cyberstrikes”, New York Times
21. Ibid.
22. Ibid.
23. NRC, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, p. viii
24. Dunlap, “Some Reflections on the Intersection of Law and Ethics in Cyber War”, p. 26
25. Ibid., p. 27
26. Ibid.
27. Brisbane Times, “Killing of Americans by Drones is Lawful”
28. Dunlap, “Some Reflections on the Intersection of Law and Ethics in Cyber War”, p. 31
29. Ibid.
30. Sanger and Shanker, “Broad Powers Seen for Obama in Cyberstrikes”, New York Times

BIBLIOGRAPHY

Brisbane Times, “Killing of Americans by Drones is Lawful”. 7 February 2013. http://www.brisbanetimes.com.au/world/killing-of-americans-by-drones-is-lawful-20130206-2dyo1.html#ixzz2KGFkATXl

CBS News, Bobb Orr, “Pentagon Expands Cyber Defense Amid Daily Attacks”, 6 February 2013, http://www.cbsnews.com/8301-18563_162-57568079/pentagon-expands-cyber-defense-amid-daily-attacks/

Dunlap, Charles J. Jr., Major General USAF Retired. “Some Reflections on the Intersection of Law and Ethics in Cyber War”. Air and Space Power Journal, January – February 2013.

Greenwald, Glenn. “Pentagon's New Massive Expansion of 'Cyber-Security' Unit is About Everything Except Defense”. The Guardian, 28 January 2013. http://www.guardian.co.uk/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-Stuxnet

National Research Council. “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”. Washington, DC: The National Academies Press, 2009.

Sanger, David E. and Shanker, Thom. “Broad Powers Seen for Obama in Cyberstrikes”. New York Times, 3 February 2013. http://www.nytimes.com/2013/02/04/us/broad-powers-seen- for-obama-in-cyberstrikes.html?_r=0

Smart, Steven J., Major, USAF. “Joint Targeting in Cyberspace.” Air and Space Power Journal, January – February 2013.

Air Force Cyberspace Technical Center of Excellence
Center for Cyberspace Research
Air Force Institute of Technology
2950 Hobson Way
Wright Patterson AFB, OH 45433

www.afit.edu/ccr

AFIT
Air Force Institute of Technology